Oil and Gas Commission
FIPA Access Assessments

This organization was listed as an independent public body at the start of 2024 under British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA) and the *Information Management Act* (IMA).

FIPA conducts empirical research as part of its program activities. Its access assessment activities are meant to monitor freedom of information. https://fipa.bc.ca/research-resources/access-assessments/

This PDF contains the requests that were sent to this public body, as well as the records that were subsequently released.

These records were originally collected as data for a more in-depth study as part of FIPA's empirical research. That involved submitting focused freedom of information (FOI) requests to determine how this public body, which we classified as part of the broader public sector, was interpreting and applying FOIPPA and IMA legislation.

That project is called *Access Regimes: Social Studies of Recordkeeping, Bureaucracy, and Secrecy under Freedom of Information Law.* Further information about that study can be found on the Open Science Foundation's registration platform.

Distinct from the original study, FIPA has also assessed whether this public body meets expectations identified in an IPSOS poll we commissioned. That poll can be found on the FIPA website here. https://fipa.bc.ca/oil-and-gas-commission/

About FIPA

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. While we are based in BC, our membership extends across Canada, and we regularly partner with organizations throughout the country.

Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information and privacy rights.

Requests sent to broader public sector organizations

Request item 1

Current organizational charts that indicate freedom of information personnel and information management personnel.

Summary

Charts that outline where freedom of information personnel and information management personnel exist within an organization.

Rational

Organizational charts help identify who is responsible for fulfilling certain obligations.

Request item 2

Delegation of authority charts for the Freedom of Information and Protection of Privacy Act.

Summary

Charts that outline who has certain powers under the Freedom of Information and Protection of Privacy Act.

Rational

Delegation of authority charts are standard instruments across the implementation of any law with delegable and discretionary powers.

Request item 3

Policies or procedures regarding freedom of information (not privacy), including policies and procedures regarding the routine release of information and proactive disclosure.

Summary

Freedom of information policies.

Rational

Policies are the core of implementing any new public initiative.

Request item 4

Final reports regarding the public body's performance reporting, program evaluations, or project implementation plans or proposals with respect to freedom of information.

Summary

Internal reports about freedom of information.

Rational

How public bodies monitor their performance matters.

Request item 5

Delegation of authority charts for the Information Management Act, as applicable.

Summary

Charts that outline who has certain powers under the Information Management Act.

Rational

Delegation of authority charts are standard instruments across the implementation of any law with delegable and discretionary powers.

Request item 6
Interoffice memoranda about freedom of information and records/information management.

Summary
Memos about freedom of information and records/information management.

Rational
Internal communications can structure organizational activity.

Request item 7
Metadata Application Profiles and records disposition models, as well associated policies and procedures and implementation plans and reports.

Summary
Metadata schemas for records management systems.

Rational
Metadata is an essential part of establishing control over records.

Request item 8
Office of primary responsibility designations/matrices.

Summary
Lists of offices responsible for certain organizational records.

Rational
Lists like this are often a reflection of the classification logics used to manage records.

Request item 9
Technical manuals for records management systems.

Summary
User manuals for records management software.

Rational
Manuals contribute to how staff interact with technology.

Request item 10
Acceptable use of technology policy instruments (where “instrument” has the same meaning as in Treasury Board Directive 1/23 and onboarding manuals.

Summary
Acceptable use of technology policies.

Rational
Acceptable Use Policies govern how employees may appropriately interact with technology over the course of their job.

Request item 11
File plans/lists/indexes and/or records management ontologies/thesauri.

Summary
Lists of regularly created files.

Rational
File lists are a prerequisite to an up-to-date file classification plan.

Request item 12
Public body self-assessments and audits/evaluations of records/information management.

Summary
Self-assessments conducted according to an internal government standard.

Rational
Regular reviews of records management is best practice in information governance.

Request item 13
Policy instruments regarding records or information management.

Summary
Records management policies.

Rational
Policies are the core of implementing any new public initiative.

Request item 14
Copies of record retention schedules.

Summary
Record retention schemas.

Rational
Retention schedules are the key instrument in asserting control over records classification and retention.

Request item 15
The public body's information resources/information asset plans/records management plans, as applicable.

Summary
Records management plans.

Rational
Records management is something that must be planned out carefully.

Request item 16
Licenses, contracts, or agreements between the public body and recordkeeping system service providers or contractors.

Summary
Contracts for recordkeeping systems.

Rational
Contracts detail roles and responsibilities with respect to system implementation and maintenance.

Request item 17

Final jobs description files for any employee who regularly performs a role or responsibility (1) in responding to a freedom of information request or (2) fulfilling public body's records/information management needs, including if those job descriptions do not explicitly mention FOI requests or records/information management.

Summary

Job descriptions for records management and freedom of information staff.

Rational

Job descriptions articulate the necessary skills and anticipated responsibilities of people charged with doing FOI or RM work.

Request item 18

Records confirming the appointment and responsibilities of subdivisional freedom of information (not privacy) or records management 'champions,' (i.e. an ambassador for records management or FOI within a particular unit, such as FOI Oversight Liaison Officers or Duty to Document Champions), if any. (If applicable roles exist, kindly include memorandums, plans, or reports issued by those persons).

Summary

Records concerning the appointment of employees responsible for promoting freedom of information and records management.

Rational

Internal promotion of FOI and RM contributes to effective implementation.

Request item 19

Organizational charts that include records/information management personnel (or the relevant organizational charts if your public body does not have dedicated RM/IM personal).

Summary

Charts that outline where freedom of information personnel and information management personnel exist within an organization.

Rational

Organizational charts help identify who is responsible for fulfilling certain obligations.

Request item 20

Final training packages (i.e. presentation slides, etc.) and training implementation history files (e.g. reports of completion, etc.) for freedom of information and records/information management, including initial training specific to FOI analysts/coordinators.

Summary

Training materials for freedom of information and records management.

Rational

Training is necessary for the successful implementation of FOIPPA and IMA.

Request item 21

internal surveys and the results of surveys concerning records/information management of freedom of information.

Summary
Surveys about records management and freedom of information.

Rational
Surveys of staff provide insight into the state of records management and freedom of information.

Request item 22
"Documenting government decisions" policy instruments (where "instrument" has the same meaning as in Treasury Board Directive 1/23).

Summary
Duty to document policies.

Rational
The Chief Records Officer has developed directives instructing public bodies to develop organization-specific policies for documenting government decisions.

Request item 23
Final Requests for Proposals concerning records management/freedom of information (not privacy).

Summary
Requests for proposals for freedom of information and records management projects.

Rational
RFPs document a public body's needs in order to identify the solutions they are seeking proposals to address.

Request item 24
Copies of checklists, forms, templates, guides and other tools used in relation to processing freedom of information requests.

Summary
-

Rational
Workflow materials for freedom of information processing.

Request item 25
Contracts and statements of work for consultant services for freedom of information/records management work.

Summary
Contracts and statements of work for consultants' work related to freedom of information and records management.

Rational
Contracts and statements of work define the boundaries of what work the public body performs and what work it relies on others' to perform.

Request item 26

Case management procedures (i.e. how analysts are assigned, what data is to be logged, how to notify program areas, etc.) for freedom of information requests.

Summary

Procedures for managing request workflows.

Rational

Case management software helps public bodies keep track of requests and organize their responses.

Request item 27

Copies of any plans or assessments done in preparation for the application of the Information Management Act (e.g. Readiness Assessments for the provision relating to document government decisions).

Summary

Reports produced to prepare to implement duty to document.

Rational

These reports established the baseline position from which duty to document was purportedly implemented.

Request item 28

Any previously unrequested/undisclosed records that assist in understanding how (1) records management is practiced in your public body, or (2) how decisions about freedom of information requests are made and how they are processed (e.g. any document, including an intranet file or records of another public body, that an employee references in the course of processing a request or describes how to apply exceptions, search for records, etc.).

Summary

-

Rational

-

PN

Pipeline Newsletter

Immersive reader

IM Corner

Frost, Mahia
Director, Records & Information Management

Privacy Management Program – officially launched!!

News from your RIS branch! This month we launched the official Privacy Management Program in the BCER.
Our privacy management program helps ensure the BCER is equipped to manage and protect any personal information in our custody or under our control. It also helps provide transparency and accountability by ensuring we document our privacy practices.
We have published resources for the BCER Privacy Management Program:

1. BCER Privacy Management Program (PMP) Plan – this plan includes the elements required for a successful privacy program – to ensure any collection, use or disclosure of personal information (PI) by employees or our contracted service providers is done in compliance with the Freedom of Information and Protection of Privacy Act (FOIPPA).

2. Privacy Impact Assessments (PIAs) - a risk assessment tool used for each initiative we undertake, PIAs identify initiatives that involve the collection, use or disclosure of Personal Information and offer solutions to keep us FOIPPA-compliant or support an acceptable level of risk. The PIA process demonstrates we have done our necessary due diligence. You can find a resource library of completed PIAs on the Energy Exchange.

3. Training (new 15 minute training video: Privacy 101) and guidance material, including FOI and Privacy Protection Guidance for Contractors

Our PIA process has been in place for a while, and most of you know if you start a new initiative, reach out to Julie Davidson. This next step of having a privacy management plan in place, guidance for contractors, and training has rounded out our program and increases staff awareness of good Privacy Practices.
Thank you for your time.

And remember – keep Privacy Protection in mind!!

From: Frost, Mahia
Sent: Thursday, December 14, 2023 4:48 PM
To: Communications
Subject: RE: Content Call for Pipeline

Below the line is the content for the IM Corner of the Pipeline. Thank you, Communications!

Happy Holidays BCER!

As you close 2023, and ready for the new year, you may be taking the time to clean up and ready your email as well. We support this, so recently provided some foundational Information Management training on transitory records: Information Management 101 - Transitory Information Training Session Recording. If you didn't come to one of the sessions, please watch the video to be sure you have a good understanding of what you can delete and what you should not.

The short version of the message is to make sure you know which records are transitory; then delete those transitory records so your inbox is more manageable, free of unnecessary clutter, and you can find what you need, when you need it.

Here are the links provided during the training:

- Information Management on the Energy Exchange
- Transitory Information Video (4 minutes)
- Email Management in an FOI World Video (5 minutes)
- Email Best Practices
- Documenting Decisions Training Video (10 minutes)
- Managing Transitory Information Guide

Cheers to you all – it's been a pleasure to work with you this year.

Mahia Frost (she/her)
Director, Records & Information Management
Mahia.Frost@bc-er.ca

Victoria
Office Address Directory
BCER Web Site

T. 250 419-4423
F. 250-419-4403

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Communications <communications@bc-er.ca>
Sent: Friday, December 1, 2023 1:14 PM
To: Lythall, Sherry <Sherry.Lythall@bc-er.ca>; Pulos, Eloise <Eloise.Pulos@bc-er.ca>; Barker, Julie <Julie.Barker@bc-er.ca>; Bates, Julia <Julia.Bates@bc-er.ca>; Kirkpatrick, Jennifer <Jennifer.Kirkpatrick@bc-er.ca>; Cave, Joel <Joel.Cave@bc-er.ca>; Boorman, Taylor <Taylor.Boorman@bc-er.ca>; Fan, James <James.Fan@bc-er.ca>; Wynne-Chesniak, April <April.Wynne-Chesniak@bc-er.ca>; Borissov, Theodora <Theodora.Borissov@bc-er.ca>; Howes, Ken <Ken.Howes@bc-er.ca>; Birk, Ravinder <Ravinder.Birk@bc-er.ca>; Mitchell, Rob <Rob.Mitchell@bc-er.ca>; Malcolm, Tim <Tim.Malcolm@bc-er.ca>; Korolek, Leslie <Leslie.Korolek@bc-er.ca>; Milner, Erica <Erica.Milner@bc-er.ca>; Clemen, Pam <Pam.Clemen@bc-er.ca>; Cepeliauskas, Anton <Anton.Cepeliauskas@bc-er.ca>; Armstrong, Peter <Peter.Armstrong@bc-er.ca>; Smith, Rob <Rob.Smith@bc-er.ca>; Mathews, Derek <Derek.Mathews@bc-er.ca>; France, Scott <Scott.France@bc-er.ca>; Frost, Mahia <Mahia.Frost@bc-er.ca>; Parfitt, Lannea <Lannea.Parfitt@bc-er.ca>; Gerlach, Lisa <Lisa.Gerlach@bc-er.ca>; Davidson, Julie <Julie.Davidson@bc-er.ca>; Keough, Dana <Dana.Keough@bc-er.ca>; Story, Robert <Robert.Story@bc-er.ca>; Fraser, Amy <Amy.Fraser@bc-er.ca>; Hewitt, Kate <Kate.Hewitt@bc-er.ca>; Bentley, Kelly <Kelly.Bentley@bc-er.ca>; Johnson, Justine <Justine.Johnson@bc-er.ca>; Rolick, Ryan <Ryan.Rolick@bc-er.ca>; White, Katelyn <Katelyn.White@bc-er.ca>; Mackay, Allison <Allison.Mackay@bc-er.ca>; Siriunas, Kristofer <Kristofer.Siriunas@bc-er.ca>; Athanasopoulos, Pana <Pana.Athanasopoulos@bc-er.ca>; Babulic, Sean <Sean.Babulic@bc-er.ca>; Charters, Megan <Megan.Charters@bc-er.ca>; Louie, Amy-Jade <Amy-Jade.Louie@bc-er.ca>; van Besouw, Jordan <Jordan.vanBesouw@bc-er.ca>; Stefik, Ron <Ron.Stefik@bc-er.ca>; Stark, Nicole <Nicole.Stark@bc-er.ca>; Grace, Chuck <Chuck.Grace@bc-er.ca>; Edgar, Matt <Matt.Edgar@bc-er.ca>; Hohnsbehn, Cathy <Cathy.Hohnsbehn@bc-er.ca>; King, Linda <Linda.King@bc-er.ca>; Mathews, Suzanne <Suzanne.Mathews@bc-er.ca>; Bhuyan, Gouri <Gouri.Bhuyan@bc-er.ca>; Nazareth, James <James.Nazareth@bc-er.ca>; Parsonage, Kevin D <Kevin.Parsonage@bc-er.ca>; O'Neill, Sean <Sean.O'Neill@bc-er.ca>; Smith, Peter E <Peter.Smith@bc-er.ca>; Workman, Bob <Bob.Workman@bc-er.ca>; Jenneson, Madison <Madison.Jenneson@bc-er.ca>; Unruh, Butch <Butch.Unruh@bc-er.ca>; Person, Darryl <Darryl.Person@bc-er.ca>; Remenda, Alicia <Alicia.Remenda@bc-er.ca>; Goldie, Lyle <Lyle.Goldie@bc-er.ca>; Paynton, Sean C <Sean.Paynton@bc-er.ca>; Scheck, Devin C <Devin.Scheck@bc-er.ca>; Anderson, Justin <Justin.Anderson@bc-er.ca>; Bromba, Rebeccah <Rebeccah.Bromba@bc-er.ca>; Rauscher, Tarilee <Tarilee.Rauscher@bc-er.ca>; Osmond, Andrew <Andrew.Osmond@bc-er.ca>; Weatherill, Shannon M <Shannon.Weatherill@bc-er.ca>; Bozarth, Donna L <Donna.Bozarth@bc-er.ca>; Calder, Shelley A <Shelley.Calder@bc-er.ca>; Stark, Ryan <Ryan.Stark@bc-er.ca>; Erickson-Fearon, Candace <Candace.Erickson-Fearon@bc-er.ca>; Wigglesworth, Zandra <Zandra.Wigglesworth@bc-er.ca>; Curnow, Nicole <Nicole.Curnow@bc-er.ca>; Jin, Genevieve <Genevieve.Jin@bc-er.ca>; Miller, Leah <Leah.Miller@bc-er.ca>
Subject: Content Call for Pipeline

Good morning,

This is a call-out for articles or information for the next edition of Pipeline, our staff newsletter.

The deadline for submissions for this edition will be **December 15th.** Please ensure you send your articles to communications@bc-er.ca

Should you have any questions, please let us know.

Thank you,

BC ENERGY REGULATOR

BCER Communications
communications@bc-er.ca

Office Address Directory
BCER Web Site

T. 250 794-5203
F. 250-794-5390

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Communications
Sent: Wednesday, September 13, 2023 11:10 AM
To: All Staff DL
Subject: TU 2023-14 BCER Increases Availability and Quality of Digital Records

Good morning,

Technical Update **2023-14 BCER Increases Availability and Quality of Digital Records** has been posted to the BCER's website and will be distributed to industry and Indigenous Nations shortly.

Thank you,

BC ENERGY REGULATOR

BCER Communications
communications@bc-er.ca

Office Address Directory
BCER Web Site

T. 250 794-5203
F. 250-794-5390

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Frost, Mahia
Sent: Tuesday, September 12, 2023 3:43 PM
To: Communications
Cc: Keough, Dana; Story, Robert
Subject: RE: Content Call for Pipeline

Hi Allison, here is our submission for September's pipeline's **IM Corner**:

I didn't have time to find a fun little graphic, so hopefully this little guidance piece is enough.

Cheers,

Mahia

Naming Conventions

Having trouble finding final versions of your documents? Are you too often scrolling through lists of documents trying to find the one you are looking for? Naming Conventions could be useful for you!

Here are some best practices:

1) Keep file and document names short and meaningful. The document name should make sense to others if the creator is unavailable.
2) Spell out acronyms unless they are very commonly known (such as BCER).
3) If using a date, use the format "Year-Month-Day" (e.g., YYYY-MM-DD or YYYY-MM or YYYY-YYYY). This will maintain chronological order.
4) Document version numbers should be indicated in the file name by using a "v" followed by the version number.
5) Include a leading zero for numbers 0-9. This will maintain numeric order. (e.g., v01, v02)
6) Avoid descriptive terms regarding format or version (e.g. Draft, Memo) at the start of file names.

We have a short guide for naming conventions on the Energy Exchange. It's high level - BCER has a wide range of functions so what works for one team may not apply to another. We recommend you have a short conversation with your team to decide what conventions would work best for you, so you are all "on the same page".

BC ENERGY REGULATOR

Mahia Frost (she/her)
Director, Records & Information Management
Mahia.Frost@bc-er.ca

Victoria
Office Address Directory
BCER Web Site

T. 250 419-4423
F. 250-419-4403

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other a recipient, please notify the sender and destroy all copies of this email immediately.

From: Communications <communications@bc-er.ca>
Sent: Friday, September 8, 2023 10:06 AM
To: Lythall, Sherry <Sherry.Lythall@bc-er.ca>; Pulos,Eloise <Eloise.Pulos@bc-er.ca>; Barker, Julie <Julie.Barker@bc-er.ca>; Bates, Julia <Julia.Bates@bc-er.ca>; Kirkpatrick, Jennifer <Jennifer.Kirkpatrick@bc-er.ca>; Cave, Joel <Joel.Cave@bc-er.ca>; Boorman, Taylor <Taylor.Boorman@bc-er.ca>; Fan, James <James.Fan@bc-er.ca>; Wynne-Chesniak, April <April.Wynne-Chesniak@bc-er.ca>; Borissov, Theodora <Theodora.Borissov@bc-er.ca>; Howes, Ken <Ken.Howes@bc-er.ca>; Birk, Ravinder <Ravinder.Birk@bc-er.ca>; Mitchell, Rob <Rob.Mitchell@bc-er.ca>; Malcolm, Tim <Tim.Malcolm@bc-er.ca>; Korolek, Leslie <Leslie.Korolek@bc-er.ca>; Milner, Erica <Erica.Milner@bc-er.ca>; Clemen, Pam <Pam.Clemen@bc-er.ca>; Cepeliauskas, Anton <Anton.Cepeliauskas@bc-er.ca>; Armstrong, Peter <Peter.Armstrong@bc-er.ca>; Smith, Rob <Rob.Smith@bc-er.ca>; Mathews, Derek <Derek.Mathews@bc-er.ca>; France, Scott <Scott.France@bc-er.ca>; Frost, Mahia <Mahia.Frost@bc-er.ca>; Parfitt, Lannea <Lannea.Parfitt@bc-er.ca>; Gerlach, Lisa <Lisa.Gerlach@bc-er.ca>; Davidson, Julie <Julie.Davidson@bc-er.ca>; Keough, Dana <Dana.Keough@bc-er.ca>; Story, Robert <Robert.Story@bc-er.ca>; Fraser, Amy <Amy.Fraser@bc-er.ca>; Hewitt, Kate <Kate.Hewitt@bc-er.ca>; Bentley, Kelly <Kelly.Bentley@bc-er.ca>; Johnson, Justine <Justine.Johnson@bc-er.ca>; Rolick, Ryan <Ryan.Rolick@bc-er.ca>; White, Katelyn <Katelyn.White@bc-er.ca>; Mackay, Allison <Allison.Mackay@bc-er.ca>; Siriunas, Kristofer <Kristofer.Siriunas@bc-er.ca>; Athanasopoulos, Pana <Pana.Athanasopoulos@bc-er.ca>; Babulic, Sean <Sean.Babulic@bc-er.ca>; Charters, Megan <Megan.Charters@bc-er.ca>; Louie, Amy-Jade <Amy-Jade.Louie@bc-er.ca>; van Besouw, Jordan <Jordan.vanBesouw@bc-er.ca>; Stefik, Ron <Ron.Stefik@bc-er.ca>; Stark, Nicole <Nicole.Stark@bc-er.ca>; Grace, Chuck <Chuck.Grace@bc-er.ca>; Edgar, Matt <Matt.Edgar@bc-er.ca>; Hohnsbehn, Cathy <Cathy.Hohnsbehn@bc-er.ca>; King, Linda <Linda.King@bc-er.ca>; Mathews, Suzanne <Suzanne.Mathews@bc-er.ca>; Bhuyan, Gouri <Gouri.Bhuyan@bc-er.ca>; Nazareth, James <James.Nazareth@bc-er.ca>; Parsonage, Kevin D <Kevin.Parsonage@bc-er.ca>; O'Neill, Sean <Sean.O'Neill@bc-er.ca>; Smith, Peter E <Peter.Smith@bc-er.ca>; Workman, Bob <Bob.Workman@bc-er.ca>; Jenneson, Madison <Madison.Jenneson@bc-er.ca>; Unruh, Butch <Butch.Unruh@bc-er.ca>; Person, Darryl <Darryl.Person@bc-er.ca>; Remenda, Alicia <Alicia.Remenda@bc-er.ca>; Goldie, Lyle <Lyle.Goldie@bc-er.ca>; Paynton, Sean C <Sean.Paynton@bc-er.ca>; Scheck, Devin C <Devin.Scheck@bc-er.ca>; Anderson, Justin <Justin.Anderson@bc-er.ca>; Bromba, Rebeccah <Rebeccah.Bromba@bc-er.ca>; Rauscher, Tarilee <Tarilee.Rauscher@bc-er.ca>; Osmond, Andrew <Andrew.Osmond@bc-er.ca>; Weatherill, Shannon M <Shannon.Weatherill@bc-er.ca>; Bozarth, Donna L <Donna.Bozarth@bc-er.ca>; Calder, Shelley A <Shelley.Calder@bc-er.ca>; Stark, Ryan <Ryan.Stark@bc-er.ca>; Erickson-Fearon, Candace <Candace.Erickson-Fearon@bc-er.ca>
Subject: Content Call for Pipeline

Good morning,

This is a call-out for articles or information for the next edition of Pipeline, our staff newsletter.

The deadline for submissions for this edition will be **Friday, Sept 15th**. Please ensure you send your articles to communications@bc-er.ca

Should you have any questions, please let us know.

Thank you,

BC ENERGY REGULATOR

From: Dickinson, Sara
Sent: Wednesday, November 29, 2023 10:51 AM
To: All Staff DL
Subject: Upcoming Training Opportunity!

Good Morning,

With just a month left in 2023 and many of us tidying up our inboxes for the new year, now is a great time to revisit our Information Management best practices.

To help staff understand how to appropriately manage, retain, and discard records at the BCER, we're hosting two workshops:

- Thursday, Dec. 7th, 1 p.m. – 2 p.m. PST / 2 p.m. – 3 p.m. MST
- Wednesday, Dec. 13th, 2 p.m. – 3 p.m. / 3 p.m. – 4 p.m. MST

These virtual workshops will cover important information, including:

- the framework for managing information in the BCER,
- the difference between transitory and official information, and
- tools and tips to make managing your information easier.

Whether you're new to the BCER, new to your role, or just need a refresher, these workshops are for you! Please keep your eyes peeled for the workshop invites and accept the time that works best in your schedule.

For more information, please visit our Information Management page on Energy Exchange. If you have any additional questions, please contact Mahia Frost.

Regards,
Sara.

BC ENERGY REGULATOR

Sara Dickinson
Executive VP, People, Reconciliation & Transformation
Sara.Dickinson@bc-er.ca

Fort St John
Office Address Directory
BCER Web Site

T. 250 794-5253
F. 250 794-5390
S17

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Frost, Mahia
Sent: Monday, July 24, 2023 8:52 AM
To: Communications
Subject: Pipeline content submission: July 24

Good morning, Communications people! Happy RAINY Monday!

Please find below this line our submission for the Information Management Corner of the Pipeline:

Welcome back to the IM Corner! This month we continue to explore the M365 tools, and best practices for using them. Here are some reminders for using OneDrive.

What are we meant to use OneDrive for?

One Drive is similar to your F: drive as your individual storage space; you are the only person with access to your OneDrive unless you grant specific permissions to a document or folder.

It is a place to store:

- transitory information (i.e., information that is not required to meet legal obligations or to sustain administrative or operational functions). Remember: Transitory information may be deleted when no longer needed.
- personal copies of HR-type records, such as your IDP
- convenience copies of reference material, and
- drafts of documents being actively worked on – until they are finalized, or ready to share with your team.

OneDrive is not an appropriate repository for long-term storage of Commission records: information is not accessible to others who may need it (such as when an employee is absent); and information is not easily searchable for FOI or legal requests. Keeping information in OneDrive creates information silos.

File critical information on OneDrive to a recordkeeping system, i.e., shared drives.

Employees are responsible for ensuring critical information that they create or receive is filed in an appropriate recordkeeping system (most often, within folders on our shared drives).

Critical Records include official or final copies, substantial drafts, correspondence, and other records that document decisions and actions.

Best practice

Regularly review your OneDrive and routinely transfer any official records to your recordkeeping system. Delete any transitory information that is no longer needed.

Consult the Official vs Transitory Records guide to learn more about what you should move to a shared drive, and what you can delete.

Energy Exchange Resource: Managing Information in OneDrive

End of submission

BC ENERGY REGULATOR

Mahia Frost (she/her)
Director, Records & Information Management
Mahia.Frost@bc-er.ca

Victoria
Office Address Directory
BCER Web Site

T. 250 419-4423
F. 250-419-4403

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Frost, Mahia
Sent: Wednesday, May 17, 2023 2:55 PM
To: Communications
Cc: Smerechinskiy, Kathryn
Subject: RE: Deadline for Pipeline Newsletter Content

Please find below this line our submission for the Information Management Corner of the Pipeline:

Welcome back to the IM Corner! This month we are sharing a reminder for using our daily tool: Teams.

Documenting Team chats

Chat messaging in Teams is an easy way to communicate with your colleagues. You can:

- send quick questions
- easily share a link
- share your priorities for the day

But if a chat strays into "official record" territory – for example, if you start making decisions that should be documented, or if the conversation is now the context for a decision, then you need to save the chat messages as a record.

You can do this in two ways:

1. create a **summary** of the conversation or decision in an email or word document, and save that to the appropriate shared drive folder; or
2. **copy the chat messages** themselves into an email or word document and save that to the appropriate shared drive folder.

Remember… Teams chats are only kept for a short time, then automatically deleted. If your chat should be part of a file, it is important that you promptly summarize or copy the chat and save the new record to its proper location on the shared drive.

Want to hear more about this? Watch our Managing Information in M365 training video, or check out our guides on the Energy Exchange.

BC ENERGY REGULATOR

Mahia Frost (she/her)
Specialist, EDRMS & Information Management Solutions
Mahia.Frost@bc-er.ca

Victoria
Office Address Directory
BCER Web Site

T. 250 419-4423
F. 250-419-4403

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other a recipient, please notify the sender and destroy all copies of this email immediately.

From: Communications <communications@bc-er.ca>
Sent: Wednesday, May 17, 2023 2:11 PM
To: Barker, Julie <Julie.Barker@bc-er.ca>; Kirkpatrick, Jennifer <Jennifer.Kirkpatrick@bc-er.ca>; Cave, Joel <Joel.Cave@bc-er.ca>; Abbott, Wade <Wade.Abbott@bc-er.ca>; Mitchell, Rob <Rob.Mitchell@bc-er.ca>; Birk, Ravinder <Ravinder.Birk@bc-er.ca>; Clemen, Pam <Pam.Clemen@bc-er.ca>; Sharma, Aashna <Aashna.Sharma@bc-er.ca>; Armstrong, Peter <Peter.Armstrong@bc-er.ca>; Smith, Rob <Rob.Smith@bc-er.ca>; Mathews, Derek <Derek.Mathews@bc-er.ca>; France, Scott <Scott.France@bc-er.ca>; Smerechinskiy, Kathryn <Kathryn.Smerechinskiy@bc-er.ca>; Frost, Mahia <Mahia.Frost@bc-er.ca>; Parfitt, Lannea <Lannea.Parfitt@bc-er.ca>; Gerlach, Lisa <Lisa.Gerlach@bc-er.ca>; Rolick, Ryan <Ryan.Rolick@bc-er.ca>; Louie, Amy-Jade <Amy-Jade.Louie@bc-er.ca>; Stefik, Ron <Ron.Stefik@bc-er.ca>; van Besouw, Jordan <Jordan.vanBesouw@bc-er.ca>; Johnson, Jeff <Jeff.Johnson@bc-er.ca>; Janzen, Mike <Mike.Janzen@bc-er.ca>; Wynne-Chesniak, April <April.Wynne-Chesniak@bc-er.ca>; Krakau, Lauren <Lauren.Krakau@bc-er.ca>; Borissov, Theodora <Theodora.Borissov@bc-er.ca>; King, Linda <Linda.King@bc-er.ca>; Hohnsbehn, Cathy <Cathy.Hohnsbehn@bc-er.ca>; Donnell, Rebecca A <Rebecca.Donnell@bcogc.ca>; Hewitt, Kate <Kate.Hewitt@bc-er.ca>; Bentley, Kelly <Kelly.Bentley@bc-er.ca>; Mathews, Suzanne <Suzanne.Mathews@bc-er.ca>; Nazareth, James <James.Nazareth@bc-er.ca>; Parsonage, Kevin D <Kevin.Parsonage@bc-er.ca>; O'Neill, Sean <Sean.O'Neill@bc-er.ca>; Workman, Bob <Bob.Workman@bc-er.ca>; Kirschner, Katie <Katie.Kirschner@bc-er.ca>; Dalton, Peter <Peter.Dalton@bc-er.ca>; Wheat, Christa <Christa.Wheat@bc-er.ca>; Paynton, Sean C <Sean.Paynton@bc-er.ca>; Scheck, Devin C <Devin.Scheck@bc-er.ca>; Dosil, Ab <Ab.Dosil@bc-er.ca>; Anderson, Justin <Justin.Anderson@bc-er.ca>; Osmond, Andrew <Andrew.Osmond@bc-er.ca>; Weatherill, Shannon M <Shannon.Weatherill@bc-er.ca>; Sutherland, Jody L <Jody.Sutherland@bc-er.ca>; Bozarth, Donna L <Donna.Bozarth@bc-er.ca>; Calder, Shelley A <Shelley.Calder@bc-er.ca>; Stark, Ryan <Ryan.Stark@bc-er.ca>; Erickson-Fearon, Candace <Candace.Erickson-Fearon@bc-er.ca>; Friedrich, Hardy <Hardy.Friedrich@bc-er.ca>; Kamp, Adam <Adam.Kamp@bc-er.ca>; Pulos,Eloise <Eloise.Pulos@bc-er.ca>
Subject: Deadline for Pipeline Newsletter Content

Good afternnoon,

This is a reminder that the deadline for articles or information for the next edition of Pipeline, our staff newsletter, is **Friday, May 19th**

Please ensure you send your articles to communications@bc-er.ca

Should you have any questions, please let us know.

Thank you,

BC ENERGY REGULATOR

BCER Communications
communications@bc-er.ca

Office Address Directory
BCER Web Site

T. 250 794-5203
F. 250-794-5390

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi acknowledge the Métis and Inuit people living across B.C.

From: Frost, Mahia
Sent: Monday, March 27, 2023 2:32 PM
To: Dosil, Ab
Cc: Villines, Marion; Smerechinskiy, Kathryn
Subject: Shared Drive Organization Projects: 2022-23 Summary
Attachments: Shared Drive Organization Project 2022-23 Year End Summary.pdf

Hello Ab,

Please find attached a year-end summary of the Shared Drive Organization Project for 2022-23.

Thank you for your support of this work; we are looking forward to working with you and the branch in the new fiscal year!

Cheers,

Mahia

BC ENERGY REGULATOR

Mahia Frost (she/her)
Specialist, EDRMS & Information Management Solutions
Mahia.Frost@bc-er.ca

Victoria
Office Address Directory
BCER Web Site

T. 250 419-4423
F. 250-419-4403

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

Shared Drive Organization Projects
2022-23 Year End Summary

This report highlights the work completed in 2022-23 for the Shared Drive Organization Project. The goal of project is to create recordkeeping systems in the shared drive environment. This puts us on the path to compliance with the Information Management Act; increases findability of Commission information; assists with business continuity through staff change; and helps us to be better stewards of the information we hold.

Our primary focus this year was to complete the Engineering Project, supporting the BCER in meeting the licensing requirements of the amended Professional Governance Act. We submitted the end of project report in December (with one outlying branch who we will work with in the next year). End of project stats for the overall Engineering project:

- Over 266,000 documents reviewed and processed
- Content reduced by 37%
- Source locations streamlined - from 112 source locations to 12 (90% reduction)
- Operational / decision material moved from F: drives to central repositories

We are now working in the People Strategy and Transformation division. We just completed a project for Strategy and Reporting, who after the reorganization were integrating three lines of business into one branch. The year concludes with project planning and analysis work for Information Systems & Technology, which will commence in the new fiscal year.

It was a productive year! Here are individual project statistics for 2022-23:

2022/2023 Year-End Report			
Project - Team Lead	% complete	Docs processed	Project highlights
Drilling and Production Jordan van Besouw	100%	31,207	30% reduction in files/documents. 20% reduction in number of folders. Integrated from 10 sources to 2.
Board Services Stacey Bligh	100%	14,808	Digital Workplace Readiness Project 10% reduction in content Classification chart created to map content to SP
Reservoir Engineering Ron Stefik	100%	91,311	52% reduction in content. Integrated records from 59 source locations to 2. Records dated to 1996 - 26 years of electronic information!
Energy Geoscience Jeff Johnson	100%	47,932	58% reduction in content. Integrated records from 27 source locations to 2.
Strategy & Reporting Josh Christenson	100%	52,437	62% reduction in content. Integrated records from 14 sources to 1 (+ Documentation publication spot).
Kelowna Engineering general/ admin folders	50%	4,949	A "side of the desk" project, cleaning up old admin folders on Kelowna's K: drive.
Information Systems & Technology Ab Dosil	1%		Planning and analysis phase in this fiscal year, project to commence in new fiscal.
Total documents processed:		**242,644**	

From: Smerechinskiy, Kathryn
Sent: Thursday, February 9, 2023 2:44 PM
To: Smerechinskiy, Kathryn
Subject: Final Wording re FIPPA - Board Governance Manual

Reference copy of Final wording provided:

Legislative Requirements relating to Communications (Email) and Records
The Regulator is an open and transparent crown corporation that is subject to legislative requirements relating to information access and records. As an agent of government, the Board and each Director are governed by applicable policies, directives and legislation relating to the public's right of access to information under BC's Freedom of Information and Protection of Privacy Act (FIPPA) and the retention of non-transitory records (records of decision) pursuant to the Information Management Act (IMA) and government's duty to document key activities and decisions.

In the course of their duties, Directors may exchange email communications and documents (records) with other Directors, employees of the Regulator and third parties using personal email accounts. Such exchanges of information fall under the control of the Regulator making them subject to FIPPA and the IMA; thus, communications and records pertaining to Board business (concerning a decision) sent or received by an individual Director may, depending on content and circumstances, be subject to disclosure under FIPPA barring any applicable exemptions. Guidance materials are available to support the Board in understanding its responsibilities.

BC Oil & Gas COMMISSION

Kathryn Smerechinskiy
Director, Records & Information Management
Kathryn.Smerechinskiy@bcogc.ca

Victoria
Office Address Directory
BCOGC Web Site

T. 250 419-4487
F. 250-419-4403
S17

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Gregory, Sara
Sent: Tuesday, February 7, 2023 10:33 AM
To: Bligh, Stacey
Cc: Smerechinskiy, Kathryn
Subject: Board emails and FOIPPA

Hi Stacey – Here are some samples that Kathryn's team provided. Sharing FYI as some might be useful in developing the manual or guidance in the future.

1. OIPC's guidance document on FIPPA and personal email use risks 1515 (oipc.bc.ca)
2. Draft policy/"Board Communications Protocol" of the Victoria Public Library (VPL) – *stipulates use of VPL Board email accounts for business only; use of personal email limited to "transitory" communications* RevisedBoardCommunicationsProtocol.pdf (vpl.ca)
3. Cooperative Boards – *guidance for Board member communications:* Cooperative Boards (sharpschool.com)
4. College of Physicians and Surgeons of BC – *Board and Committee Use of Electronic Communication Policy:* Employee Manual (cpsbc.ca)
5. School District Board of Education example: 2:140-AP1 Guidance for Board Member Communications, Include EMail Use | BPS101
6. American School Board/court ruling example: California School Board Association (csba.org) – *Guidance includes putting the onus on the board member to simply advise if they have responsive FOI records or not. BCER does this for FOI (searches conducted by program areas), but the difference is that in those cases we have the ability to have IT check our server in the event of employees who have departed, or there being any issues/doubt that an adequate search was completed.*
7. Sample "Guidance" document and a Q&A format (could be modified for the Board): instant-messaging.pdf (ipc.on.ca) and use-of-email-09062017.pdf (nyssba.org)

BC Oil & Gas COMMISSION

Sara Gregory
Vice President Legal, Regulatory & Corporate Governance
Sara.Gregory@bcogc.ca

Victoria
Office Address Directory
BCOGC Web Site

T. 250 419-4476
F. 250-419-4403
S17

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi acknowledge the Métis and Inuit people living across B.C.

This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other a recipient, please notify the sender and destroy all copies of this email immediately.

From: Piccinino, Ines
Sent: Wednesday, October 26, 2022 1:51 PM
To: All Staff DL
Subject: New Records Management Guide – Reminders when Leaving the Organization

Good afternoon, all!

As we welcome many new faces to the Commission, we are also saying goodbye to some great people who are retiring or changing jobs. Our records management processes are of critical importance in managing risks, so we have taken some time to consider how to best support both employees and managers in the exit process.

Our Records & Information Management team have put together a helpful guide which outlines responsibilities and requirements for both the departing employee and their managers and supervisors. If you have any questions about this guide or records management in general, please contact any member of the Records team who will be happy to help you.

Thank you!

BC Oil & Gas COMMISSION

Ines Piccinino (she/her)
Executive Vice President, People, Strategy & Transformation
Ines.Piccinino@bcogc.ca

Victoria
Office Address Directory
BCOGC Web Site

T. 250 419-4473
F. 250-419-4403
S17

We acknowledge and respect the many Indigenous Territories and Treaty areas, each with unique cultures, languages, legal traditions and relationshi
acknowledge the Métis and Inuit people living across B.C.

*This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other
a recipient, please notify the sender and destroy all copies of this email immediately.*

From: Keough, Dana
Sent: Tuesday, August 23, 2022 3:53 PM
To: Smerechinskiy, Kathryn
Subject: FW: FOIPPA Foundations Online Course

This is the FOI training I mentioned….

From: Carling, Emma CITZ:EX <Emma.Carling@gov.bc.ca> **On Behalf Of** Lowe, Charmaine CITZ:EX
Sent: Wednesday, April 20, 2022 12:01 PM
Subject: FOIPPA Foundations Online Course

Hello,

I am writing you today about a new, free online learning opportunity on the *Freedom of Information and Protection of Privacy Act* (FOIPPA). Launching today, *FOIPPA Foundations* is an online course that supports learners to understand their privacy and access obligations in BC.

This interactive course reflects the 2021 amendments to FOIPPA and provides learners with an overview of:

- The fundamentals of FOIPPA
- Their responsibilities under FOIPPA
- How FOIPPA applies to their work
- Their privacy and access obligations

Target audiences for the course include public body employees in the broader public sector, as well as BC government employees and contracted service providers.

Course Completion

The Ministry of Citizens' Services and Open School BC will not be tracking learner completion; however, following successful completion of the course exam, learners can download a PDF certificate. The exam consists of a 10-question quiz and may be repeated as many times as necessary to obtain a passing score of 80%.

Take the course

The course is now available online www.gov.bc.ca/privacytraining.

For additional information, please contact: privacy.helpline@gov.bc.ca.

Sincerely,

Charmaine Lowe
Assistant Deputy Minister
Corporate Information and Records Management Office
Ministry of Citizens' Services

From: Armstrong, Peter
Sent: Friday, December 10, 2021 12:43 PM
To: All Staff DL
Subject: IMPORTANT UPDATE FROM IST - One Drive

Greetings from IST

Do you know you can use One Drive to share documents with your coworkers?

If you haven't already – you can activate One Drive by selecting this icon

from your taskbar and logging on with your BCOGC credentials.

You can find training materials on all Microsoft Applications from MyOGC M365 Information and Training | MyOGC (bcogc.ca)

Here you will find a link to One Drive Introduction Documentation One Drive Introduction as well as a link to Records Management Documentation One Drive BCOGC Records Management Guide

As always if you have any questions or concerns, please let us know:

- Email: Simply send an email to servicedesk@bcogc.ca and a support request will be logged in our system.
- Phone: You can call IT at (internally) 5360 or (externally) 250-794-5360

Kind regards,
Peter

Peter Armstrong
Director, Information Technology
Peter.Armstrong@BCOGC.ca

Fort St John BC
Office Address Directory
bcogc.ca

T. 250 794-5209
F 250-794-5390
S17

This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other use by a person other than the named recipient of this communication is prohibited. If you received this in error or are not named as a recipient, please notify the sender and destroy all copies of this email immediately.

Subject: Documented Destruction of Electronic Records - feedback/working session
Location: Microsoft Teams Meeting

Start: Thu 12/9/2021 2:30 PM
End: Thu 12/9/2021 3:30 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Frost, Mahia
Required Attendees: Toma, Shannon; Smerechinskiy, Kathryn; Keough, Dana

Hello team,

I have started crafting an overview on our process for defensible destruction of electronic records. This is for a few reasons: as we progress with the shared drive organization projects we need to start actioning the final disposition folders (now that we have them); it reminds people that the destruction process applies to digital records as well; and it is a transparency piece that we should have on our intranet.

The purpose of this meeting is to talk about our process and get your input / feedback on the document. I have attached three documents to support the discussion:

1. **Destruction process – electronic records** – **for your review**. This is the overview doc of why we do this, and how to do it - aimed to keep it simple.
2. **RDA File List Template** – purely for reference. I updated our current template to encompass electronic records (basically adding a shared drive location column).
3. **How to write a Folder Report** doc – for reference as well. It's possible we could try using this for the basis of creating a file list? I am not sure if it will be easier to type them out or run this and "fix it up". Looking for your opinion / thoughts.

The overview document is only halfway there - it's SUPER drafty once we get to process, and this is the purpose of the meeting. I figure the process in place for physical records will mostly apply, but it is always good to take the opportunity to step back and make sure we are doing things the best way we can. Looking forward to chatting with you about this!

Thank you for your thoughtful review and time,

Mahia

Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Join with a video conferencing device
994240142@t.plcm.vc
Video Conference ID: 111 943 571 7
Alternate VTC instructions

Last Revised: 2021-07-21				**FILE LIST OF ELECTRONIC FILES ELIGIBLE FOR DESTRUCTION**						
OIL AND GAS COMMISSION				BRANCH:		RDA #: *Records and Information Services provides*				
Drive name	**Schedule #**	**Primary/Secondary**	**FILE ID**	**FILE TITLE (include secondary title and folder name)**	**OPR (Y/N)**	**Start Date**	**End Date**	**Retention Schedule**	**SO Date (if applicable)**	**Final Disposition Date**
						yyyy/mm	yyyy/mm		yyyy/mm	

Pages 22-23
Section 13

Folder Directory Report – folders only

1. Bring up a DOS window	<Windows symbol> R
2. Type: And press OK.	CMD.EXE
3. To change the drive address type the share letter followed by a colon And press ENTER.	eg. Q:
4. To select a folder, type "cd" followed by the name of the first folder. Repeat until you reach the folder you want to use.	eg. cd divisional operations
5. To run a directory of folders, type: **The report is not finished until the flashing stops and the drive letter shows up.**	**tree > directory.txt**

In txt document, CTRL+A
CTRL+C to copy
Open Excel
CTRL+V
AAAA – search and replace

Folder Directory Report – including documents

6. Bring up a DOS window	<Windows symbol> R
7. Open:	CMD.EXE
8. To change the drive address type the share letter followed by a colon	eg. Q:
9. To select a folder, type "cd" followed by the name of the first folder. Repeat until you reach the folder you want to use.	eg. cd divisional operations
10. To run a report, type:	dir /s /b >c:\outputfile.txt (outputfile = name of new doc)

Here are the steps for a quick cleanup of the Text file on Excel

1. Using the Find & Select feature - find ÃÄÄÄ
2. Replace with a semicolon
3. Repeat for ÀÄÄÄ and ^{3} (or any odd characters that aren't needed)
4. Highlight Column A
5. In the DATA tab, select Text to Columns
6. Choose 'Delimited', and click 'Next' (Step 1 of 3)
7. Choose 'Semicolon', and click 'Next' (Step 2 of 3)
8. Keep 'General' selected, and click 'Finish' (Step 3 of 3)

From: Dawes, Len
Sent: Monday, September 27, 2021 9:34 AM
To: All Staff DL
Subject: Managing Information in M365

In support of the Commission's ongoing transition to M365, the Records & Information Services branch has created a new training video – *"Managing Information in M365".* This training covers the basics of what we need to know for appropriately managing information in OneDrive, Teams and SharePoint applications.

Please take the time to watch this 16 minute video. It can be found on the **M365 Information and Training page** and directly accessed from **here**.

Any follow up questions about the training content can be directed to our records management support staff (Kathryn Smerechinskiy or Mahia Frost).

Thanks,

Len

Len Dawes CPA, CA
Executive Vice President, Chief Financial Officer
Len.Dawes@BCOGC.ca

Victoria BC
Office Address Directory
bcogc.ca

T. 250 419-4405
F. 250-419-4403
S17

This email and any attachments are intended only for the named recipient and may contain confidential and/or privileged material. Any unauthorized copying, dissemination or other use by a person other than the named recipient of this communication is prohibited. If you received this in error or are not named as a recipient, please notify the sender and destroy all copies of this email immediately.

ISSUANCE: **Corporate Services Division**
Records Management/Information Technology

APPROVED: **April 27, 2021**

1.0 GENERAL

1..1 Background

The BC Oil and Gas Commission (Commission) is adopting Microsoft Office 365 (M365) as a communication, collaboration and working platform. M365 provides a new suite of tools for creating, accessing, and sharing information and creates new digital workspaces.

1..2 Purpose

The purpose of this policy is to set a standard for how the Commission will use the M365 applications and appropriately manage the information residing in them. The use of M365 tools must comply with our legislative and policy requirements relating to information management and confidentiality. This means records and information stored using an M365 application or service must be:

- Appropriately retained to adequately document Commission decisions.
- Actively managed throughout their lifecycle according to retention policy.
- Secured and managed to prevent inadvertent disclosures.
- Assessed for confidentiality and, when appropriate, protected as a confidential asset.
- Readily accessible for Freedom of Information (FOI) and eDiscovery requests.

M365 is a new digital platform for the Commission and the Province, and its suitability as a corporate recordkeeping system has not yet been fully assessed. As such, this policy is deemed interim in nature and may be subject to future revisions.

- **Authorities**
  - *Information Management Act*
  - *Interpretation Act*
  - *CRO 01-2019 Documenting Government Decisions Directive*
  - *Freedom of Information and Protection of Privacy Act* (FOIPPA)
  - *Transitory Records (Schedule 102901)*
  - *Oil and Gas Regulation Operational Records Classification System (ORCS)*
  - *Administrative Records Classification System (ARCS)*
  - *Human Resources ARCS Supplement*

- **Applicability**

  This policy applies to all data, records and information stored in M365 applications.

- **Related Policy/Procedure**

  This policy, in conjunction with the following, is part of the information governance framework in the Commission:

  - *Information Management Policy*
  - *Managing Confidential Information Guide*
  - *Managing Email Guide*
  - *Employee Code of Conduct and Ethics*
  - *Information Security Policy*
  - *Mobile Device Policy*
  - *Use of IT Resources Policy*

2.0 POLICY

2.1 Records and Information Management

- Commission records and information must be consistently managed according to approved information schedules (i.e., ARCS/ORCS).
- Official records within M365 workspaces must be saved to an appropriate recordkeeping system (shared drives) to ensure Commission decisions are adequately documented and business continuity and operations are supported.
- Only transitory information may be destroyed at the discretion of the employee.

2.2 Collaboration and Protecting Confidentiality

When using M365, users must limit the sharing of sensitive or confidential information, (e.g., personal information).

- Confidential records and personal information must not be inappropriately shared in M365 workspaces. If sharing is necessary, ensure proper handling and protections are in place.
- Access to M365 workspaces will only be granted to appropriate users and groups, as determined by Team/Site Owners.
- Access permissions assigned to collaborative workspaces will be actively managed, and access will be updated in a timely manner when group composites change.
- External individuals will not be granted access to Commission M365 workspaces without prior approval by a member of the Leadership group. If permissions are granted, Team/Site owners must ensure the protection of any confidential or sensitive information in the shared environment.

2.3 Freedom of Information and legal records searches (eDiscovery)

Information in M365, like all Commission information, is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or other legal obligations. When using M365, staff must be prepared to respond to Freedom of Information (FOI) and legal requests for records and information.

Upon notification of a FOI and/or legal discovery request, users must assist in the search and retrieval of responsive records from applicable M365 workspaces, within prescribed time allowances as requested by FOI or Legal Services branch.

- Employees must not delete responsive records or information stored within M365 workspaces, including that which may be considered transitory. It is unlawful to delete or destroy any transitory record that is the subject of a current FOI request, or is subject to a current or reasonably anticipated litigation discovery process.
- Temporary holds on M365 automated information deletions should be initiated for applicable M365 applications.
- Searches for responsive records must be conducted within all applicable M365 workspaces.

3.0 APPLICATION USAGE

3.1 Teams

Teams workspace is to be used for transitory information only.

Teams is used for:

- Ad hoc informal conversations (chats) between two or more people.
- Department/branch communications.
- Project/committee/working groups.

Retention of chat messages:

- Ad hoc chat messages (outside of Teams Sites and Channels) are automatically deleted after 10 days.
- Department/branch conversations (within a Teams Site or Channel) are automatically deleted after three months.
- Project/committee/working group conversations (within Teams Sites or Channels) are kept for the duration of the project, then deleted.

Documenting decisions and capturing official information in Teams:

- Any official or critical information in Teams must be captured in the recordkeeping system.
- Team/Site Owners must confirm that all official material has been transferred to the recordkeeping system before a Team site will be deleted.

3.2 OneDrive

OneDrive is similar to the F: drive, by providing a private workspace for individual use. It is intended for short-term storage of records being actively worked on, i.e., drafting and collaborating on new documents OneDrive is not an appropriate repository for long-term storage and management of Commission records.

OneDrive workspace should only hold active records while being drafted, and transitory information.

- When a record is finalized or collaboration has completed, it should be moved to the recordkeeping system.
- Users/Supervisors must confirm any official material has been transferred to the recordkeeping system before a OneDrive account is closed/deleted.

Confidentiality and collaboration considerations:

- Care must be taken to ensure that security and permissions are closely managed for confidential information being shared for collaboration.

3.3 SharePoint

There are two main uses of SharePoint in M365. Teams uses SharePoint as the platform for sharing and collaborating on documents – each Teams SharePoint is specific only to that Team and intended for short-term use and collaborative purposes. An official SharePoint site can also be used as a broader communication tool or collaboration hub at a corporate level; content stored on such sites is typically accessed across the organization and referenced for a period of longer duration, i.e., corporate policies and planning documentation, etc.

Teams SharePoint is a workspace for transitory content.

- Official records created within this workspace must be moved out of the Teams environment and saved to the recordkeeping system.

SharePoint sites outside of Teams are typically retained for a longer duration; as such, content must be managed according to records lifecycles and retention rules.

- Initiation of a corporate SharePoint site will be done in accordance with Commission SharePoint standards.
- Site structure must align with approved information schedule classifications.
- The Commission will actively maintain documentation on the intended use, access, and permissions for every site.
- SharePoint sites may be used as a records repository provided the structure aligns with information schedule classifications.
- When a site is closed, all official records should be extracted from SharePoint and saved to the recordkeeping system.

3.4 Outlook

M365 connects to Exchange Online instead of Exchange onsite. This does not significantly change email functionality or email management requirements.

- Emails should be managed according to information schedule classification and retention rules.
- Official emails should be routinely moved to and retained in the recordkeeping system.
- Inactive mailboxes may not be deleted until the contents have been assessed and official records are retained in the recordkeeping system.

4.0 ROLES AND RESPONSIBILITIES

Leadership is responsible for:

- Leading the Commission in the appropriate usage of M365 tools.

Teams/Site Owners are responsible for:

- Assigning and managing permissions to Commission workspaces.
- Ensuring the site or group workspace is appropriately managed according to Commission policy throughout its duration.

- Ensuring official records are captured in the recordkeeping system before a site/channel/group mailbox is closed.

Each employee is responsible for:

- Understanding what constitutes an official record and what information is deemed transitory.
- Managing Commission records and information, throughout the lifecycle established in approved information schedules, as appropriate to each M365 application.
- Ensuring appropriate confidentiality measures are applied to records and information.
- Ensuring the privacy of individuals is protected and maintained when using M365 tools and applications.
- Coordinating and/or conducting records searches within M365 applications in response to an FOI and/or legal request (eDiscovery).

APPROVAL:

Paul Jeakins
Commissioner,
Chief Executive Officer

Len Dawes
Executive Vice President,
Chief Financial Officer

Ken Paulson
Executive Vice President,
Chief Operating Officer

Mayka Kennedy
Executive Vice President,
Chief Engineer

Ines Piccinino
Executive Vice President,
Legal and Regulatory Affairs

Trevor Swan
Executive Vice President,
Orphan & Liability Management

Version Control:

Document Created	Apr-21	Approved by Executive Team

Appendix A: Definitions

- **Access:** the ability or opportunity to view, study or obtain a copy of the records of the Commission. FOIPPA provides the public with a right of access to records in the custody or under the control of a public body.
- **Classification:** the process of identifying records or information in accordance with an approved information schedule. This includes determination of the function and/or subject of a record and selection of the appropriate records classification.
- **Confidential Record/Information:** is information that, if compromised, could result in serious consequences for individuals, organizations, or government. Designating information as confidential depends on factors such as the value of the information, the source of the information, and the impacts of unauthorized use, disclosure, alteration, reproduction, loss, or destruction. Confidential information requires protection against unauthorized access or disclosure.
- **Outlook:** is Microsoft's email application in M365. It supports the creation and receipt of electronic mail communication.
- **Information Governance (IG):** is fundamental to good corporate governance. It provides a framework and foundation for the control and securement of corporate records and information. It relates to the activities, policies, processes, and technologies an organization applies to maximize the value of the information it holds, while minimizing the costs and risks associated with holding it. The Commission's M365 IG Policy identifies requirements and strategies for managing content and records throughout their lifecycle using the suite of tools. The focus is on being compliant with applicable legislation and policies and enabling employees to be more collaborative and productive.
- **Information Schedules**: govern how records are organized and managed. B.C. government and broader public sector organizations use information schedules to ensure records are kept for as long as required, identify records of enduring value for preservation and ensure others are routinely destroyed when they are no longer needed.
- **Leadership Group:** Commission employees with a designation of Executive Director or higher.
- **Lifecycle**: the lifespan of information from its creation or receipt and use, through to its final disposition: destruction, transfer to the government archives or alienation.
- **Official Record/Information:** a record that documents Commission activities and decisions and does not fit the criteria of transitory records.
- **OneDrive:** cloud-based storage provided to each employee for information and materials related to their work.
- **Personal Information**: is recorded information about an identifiable individual other than business contact information. Business contact information identifies an individual in a business, professional or official capacity, and can include their name, title, business address, business telephone number, business email or business fax number. Personal information typically includes an individual's name, home address, personal email address, personal telephone number, age, gender, marital or family status, any physical or mental descriptors, information about an individual's educational, financial, criminal or employment history, personal views or opinions, and photos where individuals are identifiable. A name is considered personal under FOIPPA when, combined with other personal

information, it reveals something personal about that individual. The context in which an individual's name appears determines whether it is personal information.

- **Records/Information Management**: is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Recordkeeping System:** a shared filing system in which records are captured, protected, retained, and destroyed in accordance with approved information schedules, and the integrity of the digital government information is ensured. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and ongoing training, constitutes an appropriate system for managing Commission information. Currently the Commission's recordkeeping system consists of shared drive folders.
- **Record/Information**: is created, received, and maintained by an organization or person during business. This includes formats defined in the Interpretation Act and FOIPPA, which includes "information that is recorded or stored by any means whether graphic, electronic, mechanical or otherwise".
- **Responsive Records/Information**: all records or information that pertain to the wording and/or subject of an FOI or legal request and fit within the scope of an applicant's request. A record may be deemed responsive as a result of its creation date, its content or context, who created the record, etc.
- **Retention Rules/Schedule:** embedded in Information Schedules, retention schedules govern the life cycle of a record, or series of records, provide the length of time the record is to be retained and its final disposition - destruction or transfer to the government archives.
- **SharePoint Site:** a central repository within M365 for information, links and content which may relate to a specific group of users for a specified purpose, or as a communication "hub" for an organization. SharePoint integrates with the other M365 applications and services and is intended for communication and collaboration.
- **Team's Site (referred to as a Team within Teams):** a collaborative workspace that provides transitory chat messaging, audio/video conferencing, document and information sharing, and meeting recordings. Team sites interface with a variety of M365 applications including Outlook, and documents residing in OneDrive and SharePoint. Teams Sites are structured with Channels, which are dedicated to a purpose.
- **Teams Channels**: dedicated conversation and workspace within Teams sites, where a group of people, such as project teams, committees, working groups, departments, and branches can collaborate and communicate.
- **Teams Chats (ad-hoc):** transitory instant messaging for the purpose of informal communication between people outside of Teams channels.
- **Team/Site Owner:** a Commission employee assigned as the owner of a Team who can create Channels within their team and manage permissions for those Channels. Additionally, Team Owners can set up properties for the Team including Team name and adding apps.
- **Transitory Information**: information of temporary and/or low value that is needed for only a limited period in order to complete a routine action or prepare a subsequent record (e.g., a new version). Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions.

- **Workspace**: a broadly used term referring to M365 digital platforms where we work with records and information, such as a Teams collaboration space, SharePoint site and/or OneDrive location.

Client: BCOGC
Department: All
ORCS

File Plan Info					Configuration Info								
ORCS File Plan #	Category Name (Secondary title)	Retention length	Retention Trigger	Purview Business Rule	Business Rule Rationale	Who's using category	Category (Primary Block Title)	Sub- Category (Primary title)	Retention Label	Retention Label Notes	Retention Policy	Retention Policy Notes	Refinable String / Date
20000-02	Ad-hoc analysis projects	SO nil DE	SO: if related to a plan or policy, when it has been abandoned or approved and there is no need to reference the records; for all other ad hoc analysis projects, when it no longer has reference value	Last modified + 1 month collaboration window, retain 5 years.		Heritage Conservation Regulatory Affairs	Oil and Gas Regulation ORCS	Oil and Gas Regulation - General	20000-02 Ad hoc analysis projects				
20000-02 TECH	Ad-hoc analysis projects - technical	SO nil DE	SO: if related to a plan or policy, when it has been abandoned or approved and there is no need to reference the records; for all other ad hoc analysis projects, when it no longer has reference value	Last modified + 1 month collaboration window, retain 10 years.	10y = provides an adequate reference period for engineering / scientific / technical analysis projects.	Heritage Conservation Regulatory Affairs LNG & Research	Oil and Gas Regulation ORCS	Oil and Gas Regulation - General	20000-02 Ad hoc analysis projects				
20000-06	Notebooks	SO nil DE					Oil and Gas Regulation ORCS	Oil and Gas Regulation - General					
20000-10	Statistical and activity reports	SO nil DE	SO: when information is no longer required for statistical, reporting, or analysis purposes	Last modified, + one month collaboration window, retain 5 years.		Heritage Conservation LNG & Research	Oil and Gas Regulation ORCS	Oil and Gas Regulation - General	20000-10 Statistical and activity reports				
20000-20	Corporate Registry	SO nil DE					Oil and Gas Regulation ORCS	Oil and Gas Regulation - General					
20000-40	Compliance evaluation	SO nil DE		Last modified + one month collaboration window, retain 10 years.	10y = Megan suggestion. These may relate to investigations, which have a 15 year retention.	Heritage Conservation	Oil and Gas Regulation ORCS	Oil and Gas Regulation - General	20000-40 Compliance evaluation files			Non-compliance # is used across the commission. The nature of an archaeological non-compliance is very different than someone doing a document check with a company to send in the regulated material they are late on. Maybe two categories for this classification? Non-Compliance 5y, Non-Compliance 10y?	
20100-20	Indigenous Relations	SO nil FR			MF: checking and then fill out Heritage Conservation and this sheet	Heritage Conservation	Oil and Gas Regulation ORCS	Indigenous Relations					
20100-40	Cultural awareness and training	SO nil DE	SO: when no longer used or referenced			Idigenous Relations	Oil and Gas Regulation ORCS	Indigenous Relations					
20200-05	Cancelled, expired or refused applications	SO nil DE					Oil and Gas Regulation ORCS	Application Review					
20200-17	Cancelled / withdrawn / discarded TANC applications	CY+1y nil DE					Oil and Gas Regulation ORCS	Application Review					
20200-18	Name changes, transfers and amalgamations	CY+2y 10y DE					Oil and Gas Regulation ORCS	Application Review					
20200-19	Declined TANC applications	CY+4y nil DE					Oil and Gas Regulation ORCS	Application Review					
20200-20	Application files	SO nil SR	SO: When activity file retention has expired.	Last modied, retain 50y, review/extend until archives are ready.	Provides appropriate time to determine activity status.	Dams - Technical Compliance	Oil and Gas Regulation ORCS	Application Review					
20200-40	Application review working files	SO nil DE					Oil and Gas Regulation ORCS	Application Review					
20250-05	Borden numbers	CY+1y nil DE					Oil and Gas Regulation ORCS	Archaeological Activity Monitoring					
20250-10	Final archaeological reports	SO nil DE	SO: when no longer referenced	Last modified, retain 20y, review/ extend until archives are ready	Consistent with retention for permits	Heritage Conservation	Oil and Gas Regulation ORCS	Archaeological Activity Monitoring					
20250-20	Declined, cancelled or withdrawn archaeological applications	SO nil DE					Oil and Gas Regulation ORCS	Archaeological Activity Monitoring					
20250-25	Field visits	SO nil FR				Heritage Conservation	Oil and Gas Regulation ORCS	Archaeological Activity Monitoring					
20250-30	Heritage Conservation Act (HCA) permits	SO nil FR		Last modified, retain 20y, review/ extend until archives are ready	Draft - seperated from 20200-20 because these also hold the activity. (FR in 20200-20)	Heritage Conservation	Oil and Gas Regulation ORCS	Archaeological Activity Monitoring	2025-30 Heritage Conservation Act (HCA) permits				
20300-05	Complaints	SO nil DE					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20300-40	Enforcement case files	CY+14y nil DE					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20300-45	Compliance issue and topic files	SO nil DE					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20300-50	Compliance site inspections	SO nil DE					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20300-60	Contravention decisions	SO+10y nil FR					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20300-65	Orders	SO+10y nil FR					Oil and Gas Regulation ORCS	Compliance and Enforcement					
20550-10	Final audit reports	SO nil DE	SO: when no longer required for tracking a company's overall history of compliance with their regulatory requirements	Last Modified, 1 month collaboration window, retain 10 years	10y - aligns with final annual reports retention.	Heritage Conservation Dams - Technical Compliance	Oil and Gas Regulation ORCS	External Audit and Compliance Assessment	20550-10 Final audit reports				
20550-20	Audit working files	CY+10y nil DE	CY	Created Date, 1 year collaboration, retain for 10 years.	1 year collaboration reflects audit year working cycle.	Heritage Conservation LNG & Research Dams - Technical Compliance	Oil and Gas Regulation ORCS	External Audit and Compliance Assessment	20550-20 Audit working files				
20600-30	Facility files	SO nil FR					Oil and Gas Regulation ORCS	Facilities Regulation and Monitoring					

ORCS File Plan #	Category Name (Secondary title)	Retention length	Retention Trigger	Purview Business Rule	Business Rule Rationale	Who's using category	Category (Primary Block Title)	Sub- Category (Primary title)	Retention Label	Retention Label Notes	Retention Policy	Retention Policy Notes	Refinable String / Date
20750-05	Company correspondence	CY+9y nil DE					Oil and Gas Regulation ORCS	Incident and Emergency Reponse					
20750-07	Emergency Management BC reports	CY+1y nil DE					Oil and Gas Regulation ORCS	Incident and Emergency Reponse					
20750-20	Emergency response plans (ERP's)	SO nil DE	SO = when there have been three subsequent plans received, or when the asset that the supplemental plan relates to has had a certificate of restoration issued or remedial actions completed	Created Date, 1 month collaboration window, retain 7 years.	Emergency Plans are typically renewed every two years, 7 years provides for 3 plan cycles to be retained, per retention.	Dams - Technical Compliance	Oil and Gas Regulation ORCS	Incident and Emergency Reponse					
20750-30	Exercise evaluations	SO nil DE					Oil and Gas Regulation ORCS	Incident and Emergency Reponse					
20750-45	Incidents	SO nil DE					Oil and Gas Regulation ORCS	Incident and Emergency Reponse					
20750-50	Major incident and emergency response	SO+10y nil FR					Oil and Gas	Incident and Emergency Reponse					
20850-03	Security deposit files	SO+1y 9y DE					Oil and Gas Regulation ORCS	Liability Management					
20850-20	Corporate asset files for orphaned or at risk sites	SO nil DE					Oil and Gas Regulation ORCS	Liability Management					
20850-21	Corporate asset files for transferred assets	SO nil OD					Oil and Gas Regulation ORCS	Liability Management					
20900-20	Road files	SO+5y nil FR					Oil and Gas Regulation ORCS	Road Regulation and Monitoring					
21000-35	Pipeline projects	SO nil FR					Oil and Gas Regulation ORCS	Pipeline Regulation and Monitoring					
21100-00	Policy and procedures - final	SO 5y FR	SO: when the policy/procedure is replaced or becomes irrelevant; for policy/procedures which are required to provide point-in-time evidence, such as environmental and wildlife policy, when no longer needed to provide evidence for decisions	Last Modified, retain 10 years, review/ extend until archives are ready	10y = provides 5 years for policy / procedure to be active, and covers 5 year SA.	Heritage Conservation Reg Affairs	Oil and Gas Regulation ORCS	Policy and Procedure Development	21100-00 Policy and procedures - final				
21100-12	Process mapping data	SO nil DE					Oil and Gas Regulation ORCS	Policy and Procedure Development					
21100-20	Guideline and policy development files	SO 5y DE	SO: when the final product is approved and distributed, or abandoned, and when no longer required for reference	Last modified + 1 year collaboration, retain for 5 years.		Heritage Conservation Reg Affairs LNG & Research	Oil and Gas Regulation ORCS	Policy and Procedure Development	21100-20 Policy, guideline, and procedure development files				
21400-35	Reservoir analysis and management files	SO nil FR					Oil and Gas Regulation ORCS	Reservoir Regulation and Monitoring					
21400-40	Production allowable reports	SO 7y DE					Oil and Gas Regulation ORCS	Reservoir Regulation and Monitoring					
21600-03	General inquiries	CY+1y 2y DE					Oil and Gas Regulation ORCS	Stakeholder Relations					
21600-06	External communications	CY+3y 6y FR	CY	Created Date, 1 year collaboration, retain for 10 years, review/ extend until archives are ready		Heritage Conservation	Oil and Gas Regulation ORCS	Stakeholder Relations	21600-06 External communications				
21600-20	Annual activity reports	SO nil FR	SO: when no longer being used for trend analysis, and understanding Commission and activity history	Created Date, 1 year collaboration, retain for 10 years, review/ extend until archives are ready	11 years is consistent with external reporting and communications retention, and executive schedule.		Oil and Gas Regulation ORCS	Stakeholder Relations					
21600-25	Pre-application issues case files	SO nil DE					Oil and Gas Regulation ORCS	Stakeholder Relations					
21600-30	Communications and report development files	SO nil DE					Oil and Gas Regulation ORCS	Stakeholder Relations					
21600-35	Stakeholder issues	SO nil DE	SO: when issue is resolved or no longer topical, and when no longer needed for reference purposes	last modified + 1 year , retain for 6 year	7 years provides an adequate reference period.	Dams - Technical Compliance	Oil and Gas Regulation ORCS	Stakeholder Relations					
21600-40	Strategic engagement projects	SO+7y nil DE	SO: when project is completed, cancelled, or abandoned	Last modified + 1 year collaboration, retain for 8 years.		Reg Affairs	Oil and Gas Regulation ORCS	Stakeholder Relations	21600-40 Strategic engagement projects				
21700-20	Master licenses to cut	SO nil DE					Oil and Gas Regulation ORCS	Timber Cutting Licensing					
21900-30	Well authorization files	SO nil FR					Oil and Gas Regulation ORCS	Well Regulation and Monitoring					

Item	Approach / Decision	Rationale	Considerations / Risks		
Purview Business Rules	Create fixed retention interpretations of ARCS/ORCS retentions rather than rely on the true retentions (i.e. SO triggers).	1) if we use an SO trigger (as we initially started doing) the label isn't applied until the SO flag is activated, which means we don't have record integrity protections applied (through the Preservation Hold Library), often until end of lifecycle 2) using an interpretation will create a more active review process - essentially a "nudge" which supports more active lifecycle management than waiting for people to proactively close files. One step closer to automated.	Disposition process will have to be more consultative - the 'disposition review' will now actually be two streams of review - one to determine if the SO is actually fulfilled and another because the records have truly reached the end of their lifecycle. Communication around this will have to be super transparent, and thought put into how to identify which disposition lists meet each criteria. A fair bit of analysis will have to be applied to the disposition review process. This supports us meeting an essential criteria of a government recordkeeping system , per CRO Directive CRO 01-2019, namely: "ensure the preservation and accessibility of records over time; protect against accidental or unauthorized access, alteration, copying, movement or deletion". While also being careful to "permit the retention requirements of information schedules to be applied accurately and efficiently".	https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/organizational-structure/crown-corporations/central-agencies/cirmo-spl/cro_01-2019.pdf	https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/organizational-structure/crown-corporations/central-agencies/cirmo-spl/cro_guidelines_dgd_2019.pdf
Transitory Records	We created a set of Transitory labels that branches choose from when creating the document library (i.e. 6m/1y/18m/2y).	In an effort to have all records with retention policies applied, Transitory labels encourage and support the routine disposition of transitory material.	It does introduce transitory material into the disposition process, but since this is actually an SO retention, that's appropriate in the model we have adopted.		
Non-OPR Records	Created a series of non-OPR retention labels, to be chosen by the branch when creating the document library (i.e. 1y/3y/5y).	Because of Microsoft's hard limitation of only 1000 retention labels we decided not to create non-OPR retention labels for every records classification. Working with Pauline/GU on how to document non-OPR classification for the libraries, so we have that metadata for the future.	As long as we can record the correct non-OPR classification number somewhere this seems like a good practice, which encourages a "nudge" to dispose of non-OPR material. **Pauline looking into the best way to record this.**		
Templates					
FR Records - migration	Decided to migrate all FR records rather than leave them behind in the Shared Drives	Keeps the records requiring management together in one place.	SharePoint doesn't have an archives/transfer type of function so still need to work the process out.		
FR Records - transfer to government archives	Transfer a copy to the archives, and then unlabel the records to destroy them. Will probably create a of label named something like "FR Transferred to Archives" that we then apply so we can get rid of the records in our custody.	We will likely have a record of what was transferred, so we will have that documentation.	This will of course have to be tested out.		
Board Records	Board Records accessed from the Portal will be considered the official records of the Board. We will not declare them as Records.	The records behind the Portal reside in a locked down SharePoint library accessible only by the Corporate Governance staff. When records are transferred to the Board Portal they are in PDF form, so we have decided not to declare them as Records, as they are quite well protected already.	Corporate Governance will also have a library of Board Records on their own site - material that doesn't 'reside' in the Board Portal.		
HR Records	Use HR ARCS Supplemental for the HR Branch and use ARCS 1385-20 for the branch HR files.	This reflects the fact that the HR Supplemental was developed for agencies that don't use the PSA, which is a centralized service for HR. The ARCS classification is designed to be a "catch-all" for what is basically non-OPR files in branches.			
Templates	Classify as Transitory so people can manage them as necessary.	Templates aren't actually records, and use is too varied to determine a common retention.	May need to create a "transitory / template retention" that exceeds 18 months for nudging.		
Legal Records	Apply the OPR retention for all offices until Legal Services has a structured file system in place.	'On paper' the Legal Services branch would be the natural OPR for legal files, but the records system is pretty unstructured and left to the individual lawyers. In light of that, we will denote all of the files as OPR until we get a system in place for them.	Once we have a structured system in place we can compare branch legal files to Legal Services holdings and either change the branch files to non-OPR or designate them as DE in the disposition process (legal files are SR)		

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
20000	**OIL AND GAS REGULATION - GENERAL**				
20000-01	General	CY+1y nil DE	Creating Branch	Program Lead	
20000-02	Ad-hoc analysis projects	SO nil DE	Creating Branch	Program Lead	
20000-06	Notebooks	SO nil DE	Creating Branch	Program Lead	
20000-07	Oil and Gas Commission website	SO nil DE	Program Area updating web pages Communications	Communications Manager	Formal disposition for this classification is not implemented on a routine basis. The Communications Manager authorizing webpage updates is effectively authorizing this disposition. (see OneNote 365 notes in M365 tab re: auto-disposition)
20000-10	Statistical and activity reports	SO nil DE	Creating Branch	Program Lead	*(Covers ad hoc, statistical and routine reports (i.e. weekly/monthly/quarterly) that are not part of an operational file, such as a compliance file or well file)*
20000-20	Corporate Registry	SO nil DE	Permit Operations & Administration	Shannon Weatherill	
20000-35	OGC Board of Directors files	FY+1y 8y FR	Board Services	Stacey Bligh	
20000-40	Compliance evaluation files	SO nil DE	Creating Branch	Program Lead	*(Covers the compliance work done outside of the C&E team, or in conjunction with them)*
20100	**INDIGENOUS RELATIONS**				
20100-20	Indigenous relations	SO nil FR	Strategic Engagement	Kelly Wintemute	
20100-40	Cultural awareness and training	SO nil DE	Strategic Engagement	Kelly Wintemute	
20200	**APPLICATION REVIEW**				
20200-05	Cancelled, expired, or refused applications	SO nil DE	Permit Operations & Administration	Shannon Weatherill	
20200-18	Name changes, transfers and amalgamations	CY+2y 10y DE	Permit Operations & Administration	Shannon Weatherill	
20200-20	Applications	SO nil SR	Corporate Record	Executive	
20200-40	Application review working files	SO nil DE	Creating Branch	Program Lead	*(Covers the working files of anyone in the Commission who is part of the application review process.)*
20250	**ARCHAEOLOGICAL ACTIVITY MONITORING**				
20250-05	Borden numbers	Cy+1y nil DE	Heritage Conservation	Megan Charters?	

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
20250-10	Final archaeological reports	SO nil DE	Heritage Conservation	Megan Charters?	
20250-20	Declined, cancelled or withdrawn archaeological permits	SO nil DE	Heritage Conservation	Megan Charters?	
20300	**COMPLIANCE AND ENFORCEMENT**				
20300-05	Complaints	SO nil DE	Compliance and Enforcement	Dax Bourke	
20300-40	Enforcement case files	CY+14y nil DE	Compliance and Enforcement	Dax Bourke	
20300-45	Compliance issue and topic files	SO nil DE	Compliance and Enforcement	Dax Bourke	
20300-50	Compliance site inspections	SO nil DE	Compliance and Enforcement	Dax Bourke	
20300-60	Contravention decisions	SO+10y nil FR	Compliance and Enforcement	Dax Bourke	
20300-65	Orders	SO+10y nil FR	Compliance and Enforcement	Dax Bourke	
20550	**EXTERNAL AUDIT AND COMPLIANCE ASSESSMENT**				
20550-10	Final reports	SO nil DE	Environmental Management Systems	Nicole Curnow	
20550-20	Audit working files	CY+10y nil DE	Environmental Management Systems Integrity Management Programs Environmental Stewardship (COR) Heritage Conservation	Nicole Curnow Kevin Parsonage Devin Scheck Megan Charters?	
20600	**FACILITIES REGULATION AND MONITORING**				
20300-30	Facility files	SO nil FR	Corporate Record	Executive	
20750	**INCIDENT AND EMERGENCY RESPONSE**				
20750-05	Company correspondence	CY+9y nil DE	Security & Emergency Management	Peter Dalton	
20750-07	Emergency Management BC reports	CY+1y nil DE	Security & Emergency Management	Peter Dalton	
20750-20	Emergency response plans (ERP's)	SO nil DE	Security & Emergency Management	Peter Dalton	
20750-30	Exercise evaluations	SO nil DE	Security & Emergency Management	Peter Dalton	
20750-45	Incident files	SO nil DE	Security & Emergency Management Environmental Stewardship	Peter Dalton Devin Scheck	

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
20750-50	Major incident and emergency response files	SO nil FR	Security & Emergency Management Environmental Stewardship	Peter Dalton Devin Scheck	
20850	**LIABILITY MANAGEMENT**				
20850-03	Security deposit files	SO+1y 9y DE	Liabilities and Orphans	Brian Murphy	
20850-20	Corporate asset files for orphaned or at risk sites	SO nil DE	Liabilities and Orphans	Brian Murphy	
20850-21	Corporate asset files for transferred assets	SO nil OD	Liabilities and Orphans	Brian Murphy	
20900	**ROAD REGULATION AND MONITORING**				
20900-20	Road files	SO+5y nil FR	Corporate Record	Executive	
21000	**PIPELINE REGULATION AND MONITORING**				
21000-35	Pipeline projects	SO nil FR	Corporate Record	Executive	
21100	**POLICY AND PROCEDURE DEVELOPMENT**				
21100-00	Policy and procedures – final	SO 5y FR	Internal: Branch who "owns" the policy External: Business Process Services / Documentation	Program Lead Derek Hughson	*(Covers both internal and external policies, guides, manuals, best practices, etc.)*
21100-20	Policy, guideline, and procedure development files	SO 5y DE	Creating Branch	Program Lead	
21400	**RESERVOIR REGULATION AND MONITORING**				
21400-25	Geological topical files	SO nil DE	Petroleum Geology	Jeff Johnson	
21400-35	Reservoir analysis and management	SO nil FR	Reservoir Engineering	Ron Stefik	
21400-40	Production allowable reports	SO 7y DE	Reservoir Engineering	Ron Stefik	
21600	**STAKEHOLDER RELATIONS**				
21600-06	External communications	CY+3y 6y FR	Public & Corporate Relations	Graham Currie	

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
21600-20	Annual activity reports *(this covers all Commission reports produced on an annual basis)*	SO nil FR	Program Area who "owns" the report (for program specific reports, such as the annual archaeology rpt) Public & Corporate Relations for corporate, commission wide reports	Program Lead Graham Currie	
21600-25	Pre-application issues case files	SO nil DE	Creating Branch	Program Lead	*(Applies to landowner liaison case files and includes archaeology as well, may be Suzanne Matthews etc.)*
21600-30	Stakeholder issues	SO nil DE	Stakeholder Relations	Graham Currie	*(Covers the resolution of issues and concerns that are not related to specific permits, applications, or part of the pre-application process)* *May start to be used by other program areas for their own initiatives. If so, apply the OPR retention.*
21600-35	Strategic engagement projects	SO+7y nil DE	Stakeholder Relations	Graham Currie	
21600-40	Report development files	SO nil DE	Program area developing the annual report.	Program Lead	*(Covers the development / draft material for producing the annual reports under -20.)*
21700	**TIMBER CUTTING LICENSING**				
21700-20	Master licences to cut	SO nil DE	Permit Operations & Administration	Shannon Weatherill	
21900	**WELL REGULATION AND MONITORING**				
21900-30	Well authorization files	SO nil FR	Corporate Record	Executive	
ARCS – ONLY CLASSIFICATIONS THAT HAVE A CORPORATE OPR IN THE COMMISSION **If you have records under any of the listed classification, but aren't the listed OPR, they will be designated as non-OPR.**					
ADMINISTRATION					
105-02	Organization charts and organization histories	SO nil FR	Human Resources Branch	Angela Scammel	

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
265-20	Delegation of authority authorization records	SO+1y 6y DE	Legal Services Branch	Sara Gregory	
275-30	Business continuity plans	SO+1y 5y DE	Integrated Risk Management	Theodora Borrissov	
292-30	FOI requests and related complaints	SO 5y SR	Records and Information Services	Kathryn Smerechinskiy	
293-60	Privacy Impact Assessments	SO+1y nil DE	Records and Information Services	Kathryn Smerechinskiy	
350-20	Legal files	SO+1y nil SR	Legal Services Branch	Sara Gregory	
432-30	Destruction case files	CY+30y nil DE	Records and Information Services	Kathryn Smerechinskiy	
BUILDINGS AND PROPERTIES					
Entire section	• Accommodation planning • Building and land management • Building design and construction projects		Corporate Property & Administration	Julie Barker	
FINANCIAL MANAGEMENT As the Commission OPR for this function, the Financial & Administration Branch will be considered the OPR for financial records, including contracts. General staff in the Commission may have related records, kept for convenience, (such as contract management records), which will be designated as non-OPR. The exception to this would be if the branch has a clear co-ownership for the function, such as determination of capacity spending.					
Entire section	• accounts payable • budget development/control, • cost-sharing • procurement and contract management, • grant and other transfer payment accounting, • revenue/expenditure control, • audits and compliance reviews, • financial reporting and analysis, tax reporting		Financial and Administration Branch	Joel Cave	

BCOGC - OFFICE OF PRIMARY RESPONSIBILITY MATRIX

Classification	Classification Title	Retention	OPR	Program Lead	Notes
HUMAN RESOURCE MANAGEMENT As the Commission OPR for this function, the Human Resources Branch uses the Human Resources ARCS Supplement for their records. General staff in the Commission may use ARCS for their HR-related records (the retentions are appropriate for this) .					
INFORMATION TECHNOLOGY The Information Technology/Information Systems branches will usually be the OPR for this section of classifications. There will be exceptions - for example, there are projects where they work with other people on system development, for example, and so we aren't setting a corporate OPR for this section.					

Identify corporate OPR streams – legal, foi, accounts payable, hr etc.

BC Oil & Gas COMMISSION

MANAGING INFORMATION IN SHAREPOINT

Microsoft SharePoint

SharePoint is a document management and collaboration tool in Microsoft Office 365. It is used to collaborate and share content across an organization. It can also be used as a records management tool. This guide provides advice and guidance on using SharePoint to manage commission records.

Under *the Information Management Act* (IMA), government bodies must ensure that an appropriate system is in place for creating and maintaining government information. If managed appropriately, SharePoint can be part of that system.

Planning to implement SharePoint

Implementing a SharePoint site should involve the same careful planning as required for any system implementation. This generally includes the following steps:

A. Requirements gathering and analysis
B. Gaining and maintaining management commitment and support for the project
C. Pre-implementation architecture, design, configuration and testing
D. Establishing governance, user training, and communications protocols
E. Post-implementation testing and monitoring
F. Post-project document migration to a recordkeeping system and closing the SharePoint site

Assign responsibility for managing and filing records at the start. Do not wait until the site project/purpose is over before identifying who needs to manage and file the documents into the appropriate recordkeeping system.

SharePoint Site Owners are responsible for:

- Identifying appropriate site users and permissions.
- Creating and managing document Libraries and Content Types.
- Ensuring documents are migrated to a recordkeeping system at project completion or site closure.

This guide only applies to the M365 SharePoint application.

It does not apply to records and information in Teams.

Teams uses SharePoint for short-term collaboration. However, Teams is not an approved recordkeeping system under the IMA. Once you are finished collaborating on a document in Teams, it should be saved to your recordkeeping system.

Do not keep final document versions in Teams SharePoint for long-term storage

BC Oil & Gas COMMISSION

Site Owners are responsible to ensure information is appropriately managed in the SharePoint environment.

Using SharePoint to manage your records

There are many ways to use and configure SharePoint. The following best practices provide some basic records management measures for the records maintained there:

- **Establish and document responsibility for the site and access to it. Keep that documentation up to date.** Site Owners need to ensure all access permissions are kept current. This enables authorized staff to locate the records and information they need for operational, FOI or other legal purposes.
- **Implement an ARCS and ORCS structure upfront.** SharePoint sites should be organized according to approved information schedules (ARCS/ORCS). This involves mapping site content to specific record classifications. Contact Records and Information Services for guidance on how to do this.
- **Document design and configuration decisions.**
- **Use naming conventions for documents.** Try to consistently title documents with established naming conventions, or using standard elements (e.g. a clear description of the document, version number, and creation date).
- **Delete transitory information regularly.** Information management rules apply to records in SharePoint. Transitory records may be routinely deleted by employees. All other records must follow the retention schedules outlined in ARCS/ORCS.

FOI, Privacy and Confidentiality of Information

Information in SharePoint is subject to access requests under the *Freedom of Information and Protection of Privacy Act* (FOIPPA). When using SharePoint, ensure you:

- Are prepared to respond with copies of responsive records for FOI or other legal obligations.
- Limit sharing personal, sensitive or confidential information to only what is necessary for conducting Commission business.

Shutting down your SharePoint site?

Contact Records and Information Services first.

Your records may need to be migrated to a recordkeeping system once the site is no longer in use.
We will help guide you on the best course of action.

BC Oil & Gas COMMISSION

COMMISSION INFORMATION IN THE CLOUD

This guide will outline some of the information and records management concerns which should be addressed by government bodies when considering the use of cloud-based computing services.

Cloud computing is internet-based computing where shared resources, software and information are provided to computers and other devices on demand.

As a government body, Commission information is government information. These terms are used interchangeably in this guide.

What types of applications and services are offered?

Cloud computing refers to services provided on-demand over the Internet, such as data storage, business software, or computing power. As a user, you get access to this service without having to manage the service yourself. One common example of cloud computing is Gmail, which allows you to log in through a web browser on any device to access your emails (i.e. the data is hosted by the cloud service provider, Google).

There are many benefits to cloud computing. For example, cloud services are more efficient, scalable and highly accessible. In addition, they can provide better security since cloud providers offer security features and internationally recognized certifications that would be a challenge for any one organization to deliver on its own. Cloud solutions will help us innovate: they let us experiment with new technologies and tools without making large capital investments up front.

While cloud technology is the future of modern service delivery, cloud solutions may not be appropriate in every case. A cloud solution is only appropriate if it meets business, privacy, security and system requirements. A public body may explore and purchase cloud services, so long as they are appropriate and their intended use complies with legal and policy requirements.

Issues to Consider

Capture

The *Information Management Act* (IMA) requires that government bodies maintain an appropriate system for creating and maintaining government information.

When using Cloud services, government bodies must ensure that records are captured or created in a way that ensures their preservation and accessibility, in accordance with applicable laws and policies. Prior to entering into an agreement with a cloud provider, government bodies should consider the following:

- Records should be created in a secure and stable format so that they can be available for future reference, use and export. Choose widely-used, non-proprietary, platform-independent formats with freely available specifications where possible.
- Records creation should support authenticity and reliability. Authenticity is closely associated with the creator of a record. The name of the creator, dates of creation/ modification, unique identifiers, and electronic signatures should be documented and maintained.
- Records should be classified according to approved information schedules from creation, through their active and semi-active use to final disposition. It is very difficult to implement classification retroactively.

Under the Information Management Act, government bodies must have an appropriate recordkeeping system for managing important government information. For more information on the requirements to document government decisions see the Documenting Commission Decisions webpage.

Maintenance and Use

Cloud-based services can be used to store, maintain and use government information throughout the active and semi-active stage of its life cycle. Government bodies should ensure that:

- Information is searchable, findable and available for retrieval and re-use. Using proper records classification, file naming conventions, keywords, and logical storage structures will allow users to find and access records when needed.
- Information is authentic, reliable and free from tampering or corruption. There should be appropriate access privileges concerning the creation, modification, annotation, relocation, and destruction of records.
- Information is securely stored, backed up and managed throughout their lifecycle. This will prevent inadvertent destruction of records. If multiple copies of the same record exist, there should be established procedures that identify which record is the original, official or authoritative record.

Retention and Disposition

All government information created, stored and managed in the cloud is subject to the IMA. The Act requires that government information must be maintained in accordance with approved information schedules. In order to be in compliance with the IMA, government bodies should ensure that:

- Information is classified according to approved information schedules (i.e. ARCS/ORCS). If no information schedule exists, information must be retained until its disposition is approved by the Chief Records Officer.
- Destruction actions are authorized and reviewable.
- Destruction is automated through business rules where possible.
- Records can be maintained indefinitely if necessary (i.e. in the case of a litigation hold).
- Action or date-based retention triggers can be set.
- Deletion should apply to records, their backups and their metadata.
- Records disposal actions are documented.

Transfer / Migration / Exit

The lifecycle of cloud computing services and technologies may be much shorter than the required retention period for government information. Unless there is a clear, defined transfer/migration/exit strategy, important government information may be lost or government bodies may experience vendor lock-in. To avoid these risks, government bodies should ensure:

- There is an exit clause in the service level agreement.
- All records and associated metadata are maintained by the provider until transfer to the new system has been completed and tests carried out.
- That passwords or other forms of file-level encryption are removed.
- That records are transferred / migrated in a way that maintains their usability as records (i.e. in stable formats).
- That records are transferred / migrated in a way that maintains their authenticity, reliability and integrity (i.e. through documented procedures carried out by authorized users).

Metadata and Reporting

Government information refers to the records of government business maintained within a system, as well as the metadata associated with those records, and the audit logs created by the system. Government bodies should ensure that all metadata requirements are met by the Cloud service provider, including:

- Persistent links are maintained between the records and their metadata.
- The ability to read and write custom metadata within the system.
- The ability to comply with government metadata standards (forth coming).
- Metadata is protected from unauthorized deletion, and must be retained with the record for as long as necessary.
- Record metadata is destroyed in accordance with the record's information schedule.
- System metadata (e.g. access and audit logs) is destroyed in accordance with information schedules.

What should the Commission do when considering a cloud-based service?

When considering a cloud-based service, information management issues should be addressed very early in the adoption process. The Commission should:

- ✓ Develop procedures for how all records will be captured, managed, retained, made available to authorized users.
- ✓ Determine what information schedule applies to information going to the cloud.
- ✓ Determine which copy of records will be declared as the official, authoritative record.
- ✓ Establish and execute retention and disposition procedures in the cloud environment.
- ✓ Test transfers of records to other environments to ensure the records remain portable, reliable, authentic, trustworthy and true.
- ✓ Develop instructions on how data will be migrated, include provisions for transferring permanent records in the cloud to the government archives.
- ✓ Resolve portability and accessibility issues through good records management policies and other data governance best practices.
- ✓ Assess cloud solutions to determine if the activities require a Privacy Impact Assessment and a Security and Threat Risk Analysis - our Privacy Officers and Security Officers can help with this.

The requirements for managing government / commission information are set in the following legislation, policy and standards:

- *Information Management Act*
- *Freedom of Information and Protection of Privacy Act*
- *The Commission's Information Management Policy*
- *Administrative* and *Operational Records Classification Schedules* (ARCS and ORCS)
- *Documenting Government Decisions Directive CRO 01-2019 (Commission guidance: Documenting Commission Decisions)*
- *The Commission's Information Security Policy*

For additional Information contact Records and Information Services, or Cybersecurity, Planning & Technology.

Appendix A - Checklist for Cloud Service Contracts[1]

This checklist is a tool for assisting government bodies when assessing typical issues in boilerplate cloud computing legal agreements (contracts). This checklist also provides an overview of recordkeeping issues that are relevant to cloud computing services and should be addressed in the terms of each agreement.

	Questions	Y	N	?	Notes
1.	**Agreement**				
1.1	Is the effective start date of the agreement clearly stated?				
1.2	Is there an explanation of circumstances in which the services could be suspended?				
1.3	Is there an explanation of circumstances in which the services could be terminated? (See also Section 6)				
1.4	Is there an explanation of notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?2				
2.	**Data Ownership and Use**				
2.1	Do you retain ownership of the data that you store, transmit and/or create with the cloud service?				
2.2	Does the Provider reserve the right to use your data for the purposes of operating and improving the services?				

[1] This checklist is based on the work of the InterPARES Trust research project. For more information on issues of trust and trustworthiness of records and data in online environments see the project website.

[2] Some cloud service agreements, especially services in the public cloud, include clauses allowing the provider to change the terms of the agreement at any time at their sole discretion. Therefore, if possible, organizations should consider deleting this right, or making this right subject to the organization's agreement to any change, or ensuring the Provider is obligated to notify the organization well in advance of any changes.

	Questions	Y	N	?	Notes
2.3	Does the Provider reserve the right to use your data for the purposes of advertising?				
2.4	Does the Provider reserve the right to use, or make your data available as anonymized open data (through standard APIs)?				
2.5	Does the terms of the agreement restrict the type of content you can store with the cloud service on account of intellectual property / copyright laws?				
2.6	Does the commission hold the copyright to records that may be stored in the cloud service?				
2.7	Do the Provider's terms apply to metadata?[3]				
2.8	Do you gain ownership of metadata generated by the cloud service system during procedures of upload, management, download and migration?				
2.9	Do you have the right to access the metadata relating to your records during the contractual relationship?				
3.	**Availability, Retrieval and Use**				
3.1	Are there specific clauses regarding the availability of the service?				
3.2	Does the service ensure your data will be available when you need it?				

[3] Metadata ensure that records can be discovered, retrieved and used. They are critical for ensuring the authenticity of the record over time. They can be generated by your organization or by the Provider. It is therefore important to specifically address metadata in the contract in order to clarify issues such as ownership, access, retention and disposition during the service and after its termination.

	Questions	Y	N	?	Notes
3.3	Does the degree of availability of the data allow you to comply with freedom of information and other legislation?[4]				
3.4	Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?				
3.5	Does the degree of availability of the data allow you to comply with the right of authorities to legally access your data for investigation, control or judicial purposes?				
3.6	Are the procedures, time and cost for restoring your data following a service outage clearly stated?				
4.	**Data Storage and Preservation**				
4.1.	Data Storage				
4.1.1	Does the Provider create backups of your organization's data?				
4.1.2	If the commission manages external records (e.g. client/partner data), does the Provider create backups of that data?				
4.1.3	Do the Provider's terms apply to any backup created?5				
4.1.4	In the event of accidental data deletion, does the Provider bear responsibility for data recovery?				

[4] BC FOIPPA allows access to information held by the public body. Will the data be available to provide in the case of an access request?

[5] Notably in terms of ownership, access, security, retention and disposition during the service and after its termination

	Questions	Y	N	?	Notes
4.2.	**Data Preservation**				
4.2.1	Are there procedures outlined to indicate that your data will be managed over time in a manner that preserves their usability, reliability, authenticity and integrity? [6]				
4.2.2	Are there procedures to ensure file integrity during transfer of your data into and out of the system (e.g. checksums)?				
4.2.3	Is there an explanation provided about how the service will evolve over time (i.e. migration and/or emulation activities)?				
4.2.4	Does the system provide access to audit trails concerning activities related to evolution of the service?				
4.2.5	Will you be notified by the Provider of changes made to your data due to evolution of the service?				
4.2.6	Can you request notification of impending changes to the system related to evolution of the service that could impact your data?				
5.	**Data Retention and Disposition**				
5.1	Will your data (and all their copies, including backups) be destroyed in compliance with your information schedules?				
5.2	Will your data be immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?				

[6] Usability, reliability, authenticity and integrity might be defined in the contract (e.g., in a Definition section or in a Glossary). It is recommended to verify if your organization and the Provider have a common understanding of these concepts.

	Questions	Y	N	?	Notes
5.3	Is there information available about the nature and content of the associated metadata generated by the cloud service system?				
5.4	Will the Provider destroy associated metadata upon disposition of your data?				
5.5	Will the Provider deliver and/or give access to audit trails of the destruction activity?				
5.6	Will the Provider supply an attestation, report, or statement of deletion (if required by your internal or legal destruction policies)?				
6.	**End of Service – Contract Termination** [7]				
6.1	In the event that the Provider terminates the service, will you be notified?				
6.2	Is there an established procedure for contacting the Provider if you wish to terminate the contract?				
6.3	If the contract is terminated, will your data be transferred to you or to another Provider of your choice in a usable and interoperable format?				
6.4	Is the procedure, cost, and time period for returning/transferring your data at the end of the contract clearly stated?				
6.5	At the end of the contract, do you have the right to access the metadata generated by the cloud service system?				

[7] The end of the service is a key moment that needs to be addressed in the contract in order to specify the procedure to follow, the obligations and responsibilities of both parties and the destination of all data before the contractual relationship is terminated.

	Questions	Y	N	?	Notes
6.6	At the end of the contract and after complete acknowledgement of restitution of your data, will the service provider's copies of your data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?				
6.7	Is there an option for confirmation of deletion of records and metadata by the organization prior to termination of services with the Provider?				
6.8	Is there an option for the client to terminate the service agreement without penalty in the event that the Provider of the cloud service changes?				

Appendix B - Checklist for Retention and Disposition Functional Requirements in the Cloud[1]

This checklist is a tool for assisting ministries and agencies to assess whether proposed cloud-based storage environments will meet their information management needs, particularly when it comes to retention and disposition functionality. The checklist also provides an overview of retention and disposition issues that are relevant to systems that store government information.

	Questions	Y	N	?	Notes
1.	**Establishing Information Schedules**				
1.1	What indexing capability is supported (can it accommodate your naming conventions and classification codes for indexing)?				
1.2	Can retention periods be established (i.e. ORCS/ARCS requirements)?				
1.3	Can destruction and destruction authorization be automated?				
2.	**Applying Information Schedules**				
2.1	Can information schedules be applied to aggregations of records or data (i.e. series of documents/files/folders/tables/databases)?				
2.2	Can records be locked down for viewing only?				
2.3	Can records be retained indefinitely (i.e. in the case of a litigation hold)?				

[1] This checklist is based on the work of the InterPARES Trust research project. For more information on issues of trust and trustworthiness of records and data in online environments see the project website.

	Questions	Y	N	?	Notes
2.4	Can specific action-based disposition triggers be established?				
2.5	Can date-based disposition triggers be established?				
2.6	Can records not in an aggregation (i.e. individual files) be destroyed at a future date?				
2.7	Can records not in an aggregation be transferred out of the system at a future date?				
3.	**Executing Information Schedules**				
3.1	Can records be deleted according to information schedules?				
3.2	Can backups be deleted according to information schedules?				
3.3	Are users alerted when linked records with different retentions come into conflict?				
3.4	If more than one information schedule is associated with an aggregation of records, can multiple retention requirements be tracked to allow the manual or automatic block on the process?				
4	**Documenting Disposal Actions**				
4.1	Are disposition actions (i.e. transfer and/or deletion) documented in process metadata?				
4.2	Can all disposal actions be automatically recorded and reported to the administrator?				

	Questions	Y	N	?	Notes
5.	**Reviewing Disposition**				
5.1	Is it possible for authorized information workers to review all metadata and content?				
5.2	Can records be marked for destruction, transfer, further review?				
5.3	Are all decisions made during review stored in metadata?				
5.4	Can the system generate reports on the disposition process?				
5.5	Is there an ability to interface with a workflow facility to support scheduling, review, and export during the transfer processes?				
6.	**Integration**				
6.1	Is the metadata schema compatible with other systems, such as an EDRMS?				
6.2	Is the system able to accommodate the BC Government metadata standard? (forth-coming)				

BC Oil & Gas COMMISSION

INFORMATION MANAGEMENT IN ONEDRIVE

Microsoft OneDrive

Microsoft (MS) OneDrive is a cloud based personal workspace provided to each Microsoft 365 user for information and materials related to their work. Records within OneDrive can only be accessed by the user, unless they specifically grant permission to share a document with another person(s).

As OneDrive implementation evolves, guidance will be updated.

Recordkeeping roles and responsibilities

To comply with the *Information Management Act*, the Commission must retain all official records in an appropriate recordkeeping system.

OneDrive is not an appropriate repository for long-term storage of Commission records: information is not accessible to others who may need it (e.g. when an employee is absent); and information is not easily searchable for FOI or legal requests. Keeping information in OneDrive creates information silos.

It is intended for short-term storage of records being actively worked on, i.e. drafting a new document, or personal reference material.

Employees are responsible for ensuring critical information that they create or receive is filed in an appropriate recordkeeping system (most often, within folders on our shared drives).

Critical Records include official or final copies, substantial drafts, correspondence, and other records that document decisions and actions.

Documenting Commission Decisions

If records in OneDrive contain important decisions, or context for those decisions, they must be retained. For more information on the requirements to document decisions, see the Documenting Commission Decisions resource material.

Freedom of Information and Protection of Privacy roles and responsibilities

Information in OneDrive is subject to requests under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Freedom of Information (FOI): Employees are responsible for information searches in response to FOIPPA requests and other legal obligations within their OneDrive.

Protection of Privacy/Confidentiality: Although it is a personal workspace, OneDrive supports collaboration through the ability to share OneDrive documents through Teams or emails. When sharing a document, care must be taken to ensure sensitive or confidential material is only viewed by those who need to see it.

Limit sharing sensitive or confidential information (e.g. personal information), as you would with any communication tool; for example, when sharing a link in an email, check that only the appropriate people have access.

BC Oil & Gas COMMISSION

WHAT MUST I DO WITH INFORMATION IN ONEDRIVE?

Each employee is responsible to ensure information is appropriately managed in the OneDrive environment.

File critical information on OneDrive to a recordkeeping system, i.e. shared drives.

Because OneDrive is not an appropriate recordkeeping system, and critical information is to be filed elsewhere, OneDrive should only hold transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information may be deleted when no longer needed.

One Drive is similar to your F: drive as your individual storage space. This is a place to store information and documents that you are not ready to make official or share with your team yet, or that are for your personal use only. You are the only person with access to your OneDrive.

You can store personal copies of HR-type records, convenience copies of reference material, and drafts – until they are finalized, or ready to share with your team.

Share documents carefully.

You are responsible for managing permissions to documents you store in your OneDrive. When you select permissions, you are choosing who will be able to access your document. Only give permission to individuals who need to access the information. There are a few ways to share documents in OneDrive; be sure to select the sharing method which is appropriate to the sensitivity of the document.

Best practice

Regularly review your OneDrive and routinely transfer any official records to your recordkeeping system. Delete any transitory information that is no longer needed.

Consult the Official vs Transitory Records guide to learn more about what you should move to a shared drive, and what you can delete.

BC Oil & Gas COMMISSION

MANAGING INFORMATION IN TEAMS

Microsoft Teams

Microsoft (MS) Teams is a communication and collaboration tool in Office 365. Features include one-on-one chats, team chats, document collaboration, video meetings, and integration with other shared applications. Each MS Team has a designated Team Owner.

Page one in this guide identifies our legislated requirements and responsibilities in the Teams environment. Page two clarifies how we manage our information in Teams.

Recordkeeping Roles and Responsibilities in Teams

The Commission is governed by legislation and policy which requires us to create and keep adequate records of our decision-making and work activities.

Teams does not have the necessary functionality and controls for an appropriate recordkeeping system. It is a tool for communication and collaboration. When working in Teams:

Employees need to ensure critical information that they create in Teams is filed in an appropriate recordkeeping system (most often, this is our shared drives).

Team Owners are ultimately responsible for ensuring critical information within their Teams sites is filed in the recordkeeping system.

Critical information includes official or final copies, substantive drafts, correspondence, and other records that document decisions and actions.

You may have critical information in meeting recordings, chat messages, collaborative documents, or Planner tasks.

When documenting decisions made in Teams, remember to include the context for that decision (e.g. the discussion or chat thread that lead to the decision). For more information, see the Documenting Commission Decisions resource material.

Freedom of Information and Protection of Privacy (FOIPPA) Roles and Responsibilities in Teams

Freedom of Information (FOI):
As with all Commission records, information in Teams may be requested under FOIPPA. When working in Teams:

Team Owners, under the direction and guidance of the FOI team, are responsible for ensuring records searches are done in response to FOI requests and other legal obligations.

Employees should be prepared to respond to a records search request when notified by a Team Owner.

Protection of Privacy/Confidentiality:

Employees should try to limit sharing personal, confidential or sensitive information, as you would with any communication tool. When sharing information in Teams, remember that Team membership may change over time and include external employees or contractors.

BC Oil & Gas COMMISSION

WHAT MUST I DO WITH INFORMATION IN TEAMS?

Team Owners are responsible to ensure information is appropriately managed in the Teams environment.

File critical information from MS Teams to a recordkeeping system:

Because Teams is not an appropriate recordkeeping system, Teams primarily holds transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information is eligible for deletion when no longer needed.

Everything you do in Teams should be for collaboration purposes only. This is not a place to store documents for future use or preservation purposes. Once you are finished collaborating on a document, it should be saved to your recordkeeping system (shared drive).

Final versions of documents should not be kept in Teams for long term storage.

Manage chat messages:

Avoid using Team chats for conversation that will have operational/strategic value and must then be managed. If this happens, you must document these chat messages in a retainable format, such as a memo or email which can be stored on a shared drive:

- Copy, summarize, or transcribe the information to another document, and
- File it in your recordkeeping system.

Understand chat retentions

It is important to understand how long your chat messages remain in Teams, so that you can save critical messages in time:

- Ad hoc chat messages outside Teams channels will be deleted in 10 days.
- Department/branch Teams chat messages will be deleted from Teams after 3 months.
- Project or committee Teams chat messages remain in Teams for the duration of the project.

Save critical records from external Teams:

If you are part of a Team for an inter-jurisdictional committee, the host Team's retention rules govern the information shared in the Team space. Ensure critical records for the Commission's role in the committee are captured in the recordkeeping system.

Best Practice

Regularly review your Teams documents and chat channels, and copy out any information that is critical to your operations, or part of an official record.

Consult the Official vs Transitory Records guide to learn more about what you should move to a shared drive, and what you can leave in Teams as transitory information.

BC Oil & Gas COMMISSION

DEPARTING EMPLOYEES RECORDS MANAGEMENT GUIDE

Audience

This guide is intended for use by departing employees and their supervisors.

It outlines what needs to be done with Commission records before an employee moves on from the Commission.

Ownership of Commission Records

Digital and paper records created or received for Commission business are the property of the Commission, not of individual employees.

All business records under the control of an employee leaving the Commission must be managed (retained or disposed of) in accordance with the information schedules used by the Commission (ARCS and ORCS).

Responsibility

It is each employee's responsibility to properly manage their records prior to departure – or discuss alternate arrangements with their supervisor.

Keeping Copies

Departing employees may, with approval of their supervisor, take copies of non-confidential Commission records. (e.g. work samples) as long as consideration is given to the nature of the information and associated risks.

Employees are not permitted to take copies of any confidential records, even if transferring to another government organization.

Employee Departures

Employees should properly manage their records before departure, per the requirements on the next page.

Any **unfiled** records of a departed employee will require review and "action" – filing all official records and deleting those that are transitory in nature.

This review is typically completed by the employee's supervisor, or a designate approved by the branch's Executive Lead. Delegation will depend on the confidentiality and sensitivity of the information.

Unfiled **documents** (from an employee's F: drive or OneDrive) may be temporarily copied to a secure folder on the shared drive to support the review process.

Any unfiled **emails** in the employee's Outlook folders may be temporarily added to the email account of their supervisor (or an approved designate) for review.

Ideally, these reviews should be completed as soon as possible, to ensure important records are preserved, saved to the right location to support branch activities, and accessible to the staff that need to reference them.

Contact IT via Service Desk for assistance if there are unfiled documents or emails needing to be copied or moved to a new location for review.

Contact the Records team or check the resources on the Energy Exchange for guidance on the appropriate management of records.

BC Oil & Gas COMMISSION

PRE-DEPARTURE REQUIREMENTS

The employee and their supervisor should ensure that these requirements have been completed or, if not, that a plan is in place to complete them.

Requirements for Hardcopy (Paper) Records

Departing employees are responsible for:

- **FILING ANY OFFICAL LOOSE DOCUMENTS** stored in their office workspace into the appropriate file folder(s).
- **RETURNING** any "signed-out" files to the Records staff for re-filing (includes files retrieved from central filing/OGC File Rooms or offsite records storage facilities).
- **DESTROYING TRANSITORY RECORDS** as prescribed in the Transitory Records guides on the Energy Exchange.
- **CONSULTING WITH** and, if applicable, providing files to their supervisor prior to departure.

Requirements for E-mail and Electronic Records

Departing employees should review their email, F: drive, "desktops" and OneDrive. The records should be managed as follows:

- **FILE ALL ORIGINALS AND OFFICAL COPIES.**

  Original and official copies of records should be filed to the branch shared drive (recordkeeping system) to ensure they are appropriately protected and managed.

Originals and official copies of records may document decision-making, set policy or procedures, require a reply or action, or reflect business processes. The Email Decision Diagram and Official vs. Transitory Records guides can help you in determining what records need to be retained.

- **ENSURE ACCESSIBILITY.** Remove any encryption, passwords, or access restrictions on documents to ensure they will be accessible to authorized staff. Necessary access restrictions can be placed at a folder level in shared drives (rather than on individual documents).
- **DELETE** work-related documents that are transitory (e.g., announcements, rough notes, non-significant drafts, etc.) or that are duplicates of records already filed in the recordkeeping system.
- **DELETE** any non-work related/personal records (e.g., copy of your resume, professional association correspondence, family photographs, etc.).

If the employee cannot complete these tasks prior to departing, the supervisor may delegate them to an appropriate staff member, ensuring confidential information is protected and the branch Executive Lead approves.

BC Oil & Gas COMMISSION

Departing Employee "Action" Checklist

Hardcopy (Paper) and other Physical Records

Ensure your paper records with ongoing value are retained.

- [ ] **SHRED TRANSITORY MATERIAL**
  Place transitory paper records in locked bins for shredding.

- [ ] **FILE YOUR RECORDS**
  File your official paper records in the appropriate recordkeeping system. Label any folders/boxes of records that haven't been filed so the content can be easily determined. Notify records staff of any records ready for return to offsite storage, and return hardcopy files to central filing locations, as applicable.

- [ ] **LABEL ANY "SPECIAL MEDIA" RECORDS**
  Ensure any special media records (such as hard copy photographs, drawings, schematics, and audiovisual material) are labelled with the appropriate identifying information, such as dates, locations, names and other contextual information.

Digital (electronic) Records

Ensure your electronic records (including email) with ongoing value are retained.

- [ ] **DELETE TRANSITORY MATERIAL**
  Delete transitory emails and documents.

- [ ] **CLEAN OUT YOUR INDIVIDUAL STORAGE**
  Clean out your personal drives (F: drive and OneDrive), email accounts, etc. by filing records in the appropriate recordkeeping system (currently our shared drives), according to your branch's folder structure.

- [ ] **AVOID REMOVABLE OR PORTABLE MEDIA**
  Do not save records onto a mobile storage device (e.g., memory stick or CD); they must be stored on a Commission server that is regularly backed up and secure.

- [ ] **ENSURE DIGITAL RECORDS ARE ACCESSIBLE**
  Remove any encryption, passwords, or access restrictions on records you are filing to ensure that they are accessible to authorized staff. Discuss necessary access restrictions with your supervisor.

Leaving on Short Notice

Focus on the tasks below and advise your supervisor of what records you have, and what needs to be completed.

- [ ] **ELECTRONIC RECORDS - ORGANIZE AND IDENTIFY YOUR FILES**
  Organize and identify emails and records that have not yet been filed in the branch recordkeeping system (shared drives):
  - Group documents logically into e-folders (according to topics or broad categories)
  - Check that documents are logically named so that contents can be easily determined
  - Prepare a list, screenshot or description of your email folders, F: drive or OneDrive folders, and any other electronic records that have been your responsibility
  - Provide the information about your records, and any passwords, to your supervisor

- [ ] **HARDCOPY (PAPER) RECORDS - ORGANIZE AND/OR RETURN TO APPROPRIATE LOCATIONS**
  Complete or make arrangements for the return of any records to offsite storage or central filing/File Room, as required.

Documented Destruction Process for Electronic Records

Documenting the destruction of 'official' (non-transitory) electronic records which have reached the end of their lifecycle is a requirement in the Commission. It ensures we:

- only destroy records legally and in accordance with an approved retention schedule; and
- have an accurate and defensible records destruction audit trail.

What it means:

What is documented destruction? It is a record detailing which electronic records have been destroyed, when we destroyed them, and under what authority.

Can't I destroy anything I want? No. Commission staff may only destroy transitory records. Official Commission records need to follow the lifecycle / retention periods as set out in approved retention schedules (ARCS or ORCS) and can only be destroyed at the end of their lifecycle, after review and approval of the destruction request.

Do I have to list all documents to create this record? No. Listing is done at the folder level; we do not apply this process at the document level. Our file list template outlines the required information elements for a folder list and establishes:

- the authority for destruction (the record classification number);
- eligibility for destruction (the date range of the information); and
- the folder titles (so we know what we are destroying).

How it works:

Here is a high-level overview of the steps involved, most of which will be completed by RIS staff:

1) Create a list of the electronic files we are destroying.
2) Complete a "Request for Destruction" form.
3) Have the completed form and file list reviewed and signed off by the Program Lead (Supervisor/Director or Executive Director).
4) Submit both for approval/sign-off by the RIS branch Director.
5) Upon receipt of approval, delete the records.
6) Record the records deletion date for the destruction file.

Destruction will always be suspended if the records are relevant to an FOI request, active investigation, legal discovery, or pending litigation.

Destruction can also be suspended if other concerns apply, such as changing mandates or regulatory requirements, or a changed use or operational need for the records.

The reason for the suspension will be documented, and all related destruction activity put 'on hold' until such time as it is considered appropriate to proceed.

For more information, please contact Records and Information Services (RIS).

Practical Guidance for the BC Energy Regulator's Board of Directors

Legislative Requirements relating to Board Communications (Email) and Records

Introduction

The Regulator is an open and transparent crown corporation that is subject to legislative requirements relating to information access and records. As an agent of government, the Board and each Director are governed by applicable policies, directives and legislation relating to the public's right of access to information under BC's Freedom of Information and Protection of Privacy Act (FIPPA) and the retention of non-transitory records (i.e., records of decisions) pursuant to the Information Management Act (IMA) and the duty to document key activities and decisions.

In the course of their Board-related duties, Directors may exchange communications and documents (records) with other Directors, employees of the Regulator, and third parties using personal email accounts. Such exchanges of information fall under the control of the Regulator making them subject to FIPPA and the IMA, so it is important to manage these records appropriately. The following information has been prepared to support Directors in understanding and meeting their legislated responsibilities in relation to these Acts.

Records and Information Management

Definitions:

Term	Description
Government record	All recorded information created or received by government bodies while conducting business activities and maintained as evidence of those activities, regardless of their digital or physical format. Under the Interpretation Act, a record includes "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise."
Transitory records	Records of temporary usefulness that are not required to support or document the Regulator's business or decision-making activities. As with all records, they can exist in any format or medium (e.g., paper or electronic). Transitory records can be deleted or destroyed when no longer needed for reference purposes. Examples of transitory records include:

	• Emails, correspondence and attachments that do not document a business activity or decision (i.e., message content lacks substance). • Drafts of documents with no significant annotations, comments, approvals, or substantial changes. • Reference copies (e.g., for meetings) not needed as evidence of decisions, actions, or consultation. • Rough notes and working materials. • Published or unsolicited information from external sources (e.g., advertisements, newspapers, magazines, spam, junk mail, unsolicited correspondence not used for any business decisions or actions). IMPORTANT: Transitory records cannot be destroyed if an FOI request has been received or eDiscovery initiated, and the records relate to the topic or specified date range.
Non-transitory (Official) records	It is important to understand which records are not transitory. Non-transitory (official) records need to be filed in an appropriate recordkeeping system (e.g., a secure system maintained by the BCER's Corporate Governance branch). If any of the criteria below applies to a record, the information is NOT transitory and should be kept: • Record supports or provides evidence of a key decision (i.e., of the Board) • Record is required to meet legal or financial obligations • Record is needed to sustain the Regulator's operations, programs or administration • Record is integral to a case (i.e., needed as context for related records in a case file) • Record is needed for accountability purposes
Custody (of a record)	Having physical possession of a record, even if a public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.
Control (of a record)	Having the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure.

Director Responsibilities under the IMA:

Use of Personal Email

- Directors use personal email accounts to exchange information with other board members, employees of the Regulator or third parties.
- Emails related to the business of the Regulator's Board should be kept separate from other types of communications; it may be helpful to:
  - save them in a separate folder; and
  - include a standardized subject line in emails to make them easily identifiable and searchable (e.g., BCER: Q2 Financial Statements).

- Transitory emails should be routinely deleted when no longer required for reference. This should include deleting them from both the "inbox" and "deleted items" (trash) folders.
- Transitory records that have not been deleted could be subject to an FOI request or eDiscovery. These records cannot be legally destroyed if an FOI request has been received or eDiscovery initiated and the transitory records relate to the requested information.

Duty to Document

- The Regulator must follow government's "duty to document" directive and maintain adequate records of decisions which includes Board records. Refer to government's video on Documenting Government Decisions for more information about this requirement.
- The Board Secretary maintains official records of the Board on behalf of the Regulator.
- If a Director creates or receives a communication (e.g. from another Director or third party) that supports board business or provides evidence of board decision-making, a copy of the email and any attachments should be forwarded to the Board Secretary for filing as such records are not in the Regulator's custody (and thereby inaccessible) but are under its "control".

Access to Information / Freedom of Information

Definitions:

Term	Description
Freedom of Information (FOI) Request	An FOI request is a formal process to ask for information that falls under the custody or control of a provincial public body. A request must be made in writing and typically relates to specific information held by a public body about an individual (their personal information) or pertaining to its business activities and mandate.
Exceptions to Disclosure	FIPPA establishes an applicant's right to access records held by a public body, however there are certain exceptions to accessing records. Not all requested information is deemed appropriate for public release. Some exceptions to disclosure are mandatory (information that meets the criteria must be protected), while others are applied to requested information at a public body's discretion.

Director Responsibilities under FIPPA:

Responding to an FOI Request

- FOI requests typically follow a 30-business day processing timeline.
- When the Regulator receives an FOI request, a formal process is followed:
  1. The first step involves interpretation of the request (i.e., understanding what information an applicant is seeking) and identifying all locations where responsive records may reside.
  2. If responsive records could reasonably include communications held by Directors in their personal email accounts, the Board Secretary will send a "Call for Records" to each Director on behalf of the Regulator's FOI staff.
  3. The Call for Records is an email that includes the wording of the request, the applicant "type" (e.g., media, law firm, etc.) and any pertinent details to support the search for records.
  4. Directors will be requested to provide the Board Secretary with copies of records, should they exist, that they believe may be responsive to the request.

- An FOI request does not automatically result in the release of information; a line-by-line review of each responsive record in an FOI package is completed by the Regulator's FOI staff to identify information that should be fully or partially withheld (protected) under FIPPA's exceptions to disclosure.
- Prior to any release of information, FOI packages are reviewed by select members of the Leadership group.
- Once all Leadership feedback and approvals have been received, an FOI package is signed off by the Executive Vice President, People, Strategy & Transformation (FIPPA Delegated Head); the Board may be briefed on a request as appropriate.
- Records are then released to the applicant within the legislated timeframe for response.

FOI Request Process Flowchart

FIPPA's Exceptions to Disclosure

Section	FIPPA Section Title	Description of Exceptions to Disclosure	Application
12	Disclosure Harmful to Cabinet Confidences	Information that would reveal Cabinet confidences (e.g., advice, recommendations, policy considerations, legislation or regulations submitted or prepared for submission).	Mandatory
13	Disclosure Harmful to Policy Advice, Recommendations or Draft Regulations	Information that would reveal advice or recommendations. This section is intended to allow for full and frank discussion of policy issues during deliberative processes.	Discretionary
14	Disclosure Harmful to Legal Advice	Communications between a public body and its legal counsel to protect solicitor-client privilege.	Discretionary
15	Disclosure Harmful to Law Enforcement	Information that could harm a law enforcement matter.	Discretionary
16	Disclosure Harmful to Intergovernmental Relations or Negotiations	Covers matters that could harm the relations between BC levels of government and governments from other provinces and jurisdictions (e.g., Government of Canada, council of municipality, regional district board, aboriginal government, government of a foreign state, international organization of states).	Discretionary
17	Disclosure Harmful to Financial or Economic Harm	Information which could cause financial or economic harm to a public body or to the government.	Discretionary

18	Disclosure Harmful to Conservation of Heritage Sites	Information about heritage sites which would result in the exploitation or destruction of those sites.	Discretionary
18.1	Disclosure Harmful to Interests of an Indigenous People	Information that could reasonably be expected to harm the rights of an Indigenous People to maintain, control, protect or develop their cultural heritage, traditional knowledge, traditional cultural expressions, or manifestations of sciences, technologies, or cultures.	Mandatory
19	Disclosure Harmful to Individual or Public Safety	Information that could result in harm to any person's mental, physical, or emotional health or to public safety.	Discretionary
20	Information that will be Published or Released within 60 Days	A public body may withhold information from an applicant if it is already for sale to the public, or if the public body plans to release or publish the information within 60 days.	Discretionary
21	Disclosure Harmful to Third Party Business Interests	Public bodies are often in possession of commercial or financial information related to outside businesses and must withhold that information from an applicant if release would cause harm to the business. A three-part test must be met for a public body to appropriately apply section 21.	Mandatory
22	Disclosure Harmful to Personal Privacy	Personally identifiable information must be protected. Except in limited circumstances, a public body must not release an individual's personal information without their explicit consent.	Mandatory

Additional Resources (available soon on the Board Portal)

- Video: Transitory Records
- Video: Email Management in an FOI World

Fort St. John Records Centre Guide

The FSJ Records Centre is a secure, centralized file room that manages and stores the BCER's historical paper records and physical files. The facility is in Room 121 of the Fort St John office and has onsite records management staff that coordinate and oversee the records program. The Records Coordinators are available to provide daily assistance and support with access, use and disclosure to internal and external stakeholders of both the historical paper files and electronic data.

The Records Centre provides access to BCER staff, industry and the public to historical paper records and electronic data, including:

- OGC application files
- Well authorization files
- Pipeline and facility files
- Land tenure files
- Water licenses
- Master Licenses to Cut
- Petroleum Development Road (PDR) files
- Road Use Permits (RUP)
- Waste Management files

The Records Centre is 3800 square feet and holds over 350,000 physical files.

Requesting Files

To request files, submit a ServiceDesk request to fileroom@bc-er.ca. Records staff will retrieve the files for you and assign them to your custody. You will be notified via ServiceDesk when your files are ready to be picked up.

Files can be picked up from the Records Centre pickup shelf outside of the Records Centre. Upon request, files can be scanned and provided electronically for staff who are not in the FSJ office or when otherwise requested.

Best Practices for Records Custody

Records are valuable assets of BCER. It's important that they can be located if they're needed for time-sensitive, operational, or legal reasons.

Good records management not only helps protect records but also reduces legal risks and enhances operational efficiency.

- Once files are signed out in your name, you are responsible for them until they are returned to the Records Centre.
- Passing a file along to a co-worker? Email fileroom@bc-er.ca and have Records staff assign it to the person who will take custody of it.

- Files stored in offices or cubicles should be kept in an accessible location and clearly visible in the event that the file is required by the Records team or another BCER staff member.
- When you are finished with a file, promptly return it to the cart located directly outside of the Records Centre.

Leaving the BCER?

All files and records in your custody should be returned to the Records Centre prior to your departure. If another person will need the files, let records management staff know and they will assign the files to that person's custody. Further guidance can be found on the Records and Information Services (RIS) SharePoint: *Records Management Guide – Reminders When Leaving the Organization*.

Confidentiality and Privacy

Records assigned to you may contain sensitive or confidential information that is protected from disclosure pursuant to a defined legislative framework, multiple acts, and associated regulations.

All BCER employees have a responsibility to appropriately manage and protect confidential information.

Records held by BCER are subject to various legislation and policies, including:

Freedom of Information and Protection of Privacy Act (FOIPPA); *Information Management Act* and associated directives; *Oil & Gas Activities Act*; BCER's *Information Management Policy*; and the BCER's *Commission Code of Conduct and Ethics*.

Tips for protecting the confidentiality of paper files:

- Protect confidential information while in transit or outside of the office; do not leave files unattended or in plain view (for example, in the backseat of your car).
- If you're working with files at your home office, ensure that they are not accessible to household members or guests.
- Prior to sharing records outside the BCER, obtain the appropriate authorization and confirm with Records staff whether the records contain any confidential information. Records staff will review the records before disclosure and prepare them for public release.

For more information on working with confidential records and documents, see the BCER's *Managing Confidential Information Guide*.

If you have any questions or would like to request a file, email fileroom@bc-er.ca

Transitory Information Quick Tips

Not all BCER information needs to be retained. These quick tips will help you identify information that is transitory and understand your responsibilities as an employee. For in-depth guidance, see the Transitory Information Guide.

What is Transitory Information:

Information is transitory if it is not required to support or document the Regulator's actions and decision-making. Transitory information is information of temporary usefulness that is only needed to complete a routine action or prepare a subsequent record (such as a new version).

Content and context determine whether recorded information is transitory, not its format or medium. Just like other records, transitory information can exist in any format (paper or digital) and can be created and shared over a variety of media (e.g., email, social media, handwritten notes, voice mail, MS Teams, SharePoint, wikis, digital systems).

See the next page for common categories of transitory information.

What is Not Transitory Information:

It is important to understand which records are not transitory. Critical information, such as documentation of decisions, needs to be filed in an appropriate recordkeeping system organized according to the relevant information schedule (ARCS/ORCS)

Consider if the record is:

- ☐ required to document a decision?
- ☐ required to meet legal or financial obligations?
- ☐ needed to sustain BCER operations, programs, or administration?
- ☐ integral to a case (i.e., needed as context for related records in a case file?)
- ☐ needed for accountability purposes?
- ☐ covered by an information schedule (such as ARCS or ORCS)?

If you answer "yes" to any of these questions, the information is NOT transitory.

DO NOT destroy any transitory information that:

- May be relevant to a Freedom of Information (FOI) request or legal discovery, or
- Is stored in backup systems, which are an essential part of protecting government's information assets (i.e., triple deleting is not allowed).

Common Categories of Transitory Information

What	Features	Examples
1. Transitory Messages (such as emails, Teams chats, voice mail)	Messages and attachments that do not document a business activity or decision (i.e. message content lacks substance).	• Correspondence about meetings • Announcement of a social event • "cc" and "FYI" messages • Message about drafts and revisions
2. Transitory Drafts	Drafts with no significant annotations, comments, approvals, or substantial changes.	• Draft with minor edits and formatting updates, but no changed content • Incomplete draft that has been superseded by later versions
3. Transitory Rough Notes and Working Materials	Information used to support projects and develop official records.	• Summary of an official record • List of ideas or suggestions • Flipchart pages (and other brainstorming records)
4. Transitory Copies	Copies not needed as evidence of decisions, actions, or consultation.	• Convenience copy for a meeting • Partial copy / extract • Supplies of reports, flyers or forms
5. Transitory Systems Information	Information that is no longer needed after it is entered into systems or generated as output. Unneeded systems and internet usage documentation.	• Cookies • Data input forms • Internet browing history • System output created for reference or for providing to clients
6. Transitory Information from External Sources	Published, solicited and unsolicited items that have been: • Only used for reference, • Referred to another office, or • Returned to sender	• Advertising in various formats – pamphlets, catalogues, DVDs • Newspapers and magazines • Spam or junk mail • Unsolicited correspondence not used for any actions or decisions • Information redirected to the appropriate office (such as a forwarded email) • Confidential information returned to sender
Dispose of transitory information as soon as you are finished with it.		

NAMING CONVENTIONS FOR ELECTRONIC FILES AND FOLDERS

File and folder naming conventions are critical to maintaining well-organized electronic records. Naming documents consistently and logically distinguishes them from one another, and simplifies finding the right documents when you need them. This tip sheet provides examples of naming conventions. Each team may determine its own file naming procedures, as long as it is applied consistently.

Benefits of consistent naming are:

- Files are easily distinguished from one another
- File names are easier to browse
- Consistent naming reduces storing duplicate items (e.g., duplicate items with different names)
- Files are easier to find and access for all users (not just the file's creator)

BEST PRACTICES

1. **Keep file and document names short and meaningful.**
   The document name should make sense to others if the creator is unavailable.

2. **If using a date, use the format "Year-Month-Day"** (e.g., YYYY-MM-DD or YYYY-MM or YYYY-YYYY)
   This will maintain chronological order.

This:	Not This:
2006-03-24 Agenda	1 Feb 2007 Agenda
2006-03-24 Attachment	24 March 2006 Agenda
2006-03-24 Minutes	24 March 2006 Minutes
2007-02-01 Agenda	February 1, 2007 Minutes
2007-02-01 Minutes	March 24, 2006 Attachment

3. **Include a leading zero for numbers 0-9.**
   This will maintain numeric order.

This:	Not This:
Office Procedures v01	Office Procedures v1
Office Procedures v02	Office Procedures v10
Office Procedures v03	Office Procedures v2

4. **Order the elements in a file name according to the way the file/document will be searched for.**
   If records are retrieved according to their date, that element should appear first. If they are retrieved according to their description, that element should appear first.

Tip: File names relating to recurring events (e.g., meeting minutes, regular reports) should include both the date and the event.

When deciding the order of the elements, "date" first will usually be appropriate for events that are time specific and recurring. "Event" first will usually be appropriate for events that are infrequent.

This:	Not This:
/.../Technology Steering Committee	**/.../Technology Steering Committee**
2007-01-20 Agenda	Agenda 1 Feb 2007
2007-01-20 Minutes	Agenda 20 Jan 2007
2007-02-01 Agenda	Minutes 1 Feb 2007
2007-02-01 Minutes	Minutes 20 Jan 2007
This:	**Not This:**
/.../Events	**/.../Events**
OGC 20th Anniversary Celebration 2018-06-05	2018-06-05 OGC 20th Anniversary Celebration
Japanese Delegation Visit 2007-02	2007-02 Japanese Delegation Visit

5. **Avoid descriptive terms regarding format or version (e.g. Draft, Memo) at the start of file names.**

This:	Not This:
/.../Communications Project/	**/.../Communications Project/**
Advertising Draft	Draft Advertising
Advertising Final	Draft Budget Report 2006-2007
Budget Report 2005-2006 Final	Final Advertising
Budget Report 2006-2007 Draft	Final Budget Report 2005-2006
Grant, S	Memo Anne Thomas
Thomas, A	Memo S. Grant

Tip: For personal names, use the family name at the start of file name and use a standard format for first names.

6. **Document version numbers should be indicated in the file name by using a "v" followed by the version number.**

This	Not This
Org Chart 2006 v02	Org Chart 2006
Org Chart 2006 v03	Org Chart 2006 rev
Org Chart 2006 v04	Org Chart 2006 rev2

Adapted from York University's Tip Sheet 6 – Naming conventions for Electronic Files and Folders

EMAIL BEST PRACTICES

In our busy days, managing email records is a challenge. That said, we each have a responsibility to manage our own emails in a compliant manner. The following best practices should help you.

1. Keep messages professional

- Emails can be requested under Freedom of Information (FOI).
- Emails can be requested under litigation.
- Keep in mind that your emails could be made public or used for legal purposes.

2. Keep messages to a single topic

- Create separate messages for separate topics.
- Don't mix personal messages with business messages.
- Create a new email with separate message when an email chain starts to address more than one topic.

3. Be specific in the subject line

- Create a clear and descriptive subject title/line.
- Give recipients enough information to quickly manage the email.
- Use the title to indicate actions, purpose and any due dates or status of actions. For example, emails labelled 'FYI', 'work/life' or 'Thank You!' can generally be treated as transitory records, while those flagged 'Answer, 'Question', 'As Requested', or 'Follow up' will often need to be kept and filed.

Standard Email Subject Keywords			
Action by <date>	Work/Life	Question:	As Requested:
FYI:	Heads up:	Answer:	As Promised:
Phone msg:	Follow up:	Request:	Thank you!

4. Limit the number of copies and recipients

- Limit main recipients to those expected to take action or make decisions based on message content.
- Use 'cc' option when sending messages to recipients for informational purposes only (i.e., if recipient does not need to comment, retain or reply to the message).
- Avoid using the 'reply all' function except in cases where each member on the distribution list needs to receive the message.

5. Limit the use of attachments and graphics

- Whenever possible, post an attachment to a shared location (e.g. shared drive folder) and send a hyperlink pointing to the document's location.
- Send attachments only to those individuals who require a copy of the document (i.e., avoid using large distribution lists and the reply-to-all icon).

6. Manage email discussion chains

Email discussion generally include previous text from the various senders and recipients to the discussion. This practice creates a complete record, but can be difficult to manage as new discussions and topics emerge during the exchange of emails. Here are some methods for managing chains:

- Indicate if no reply is needed.
- Do not re-send attachments with a reply unless it is necessary.
- Stay on topic. Don't add unrelated material - if the discussion changes significantly, create a new email instead.

7. Eliminate junk mail and transitory records

- Delete messages that are only of temporary usefulness (i.e., transitory messages). These messages are typically needed a short period of time and are not required to document Commission business.
- Promptly dispose of junk mail and personal emails. Neither should remain for long on the Commission email system.

8. File official email and attachments (non-transitory)

- File official email and attachments within your office recordkeeping system – this is usually your team's shared drive folders, or may be into a system of record, such as AMS.

Not sure how to file an email into a shared drive?
There are a few ways. You can simply drag and drop the email into the appropriate folder.
Or you can copy it in Outlook and Paste it into the appropriate folder.
See our *Email Tip: How to save Emails to a Shared Drive* for more details.

- Once the official copy is filed, the source record/email (i.e. the copy in your Outlook) may be treated as redundant and deleted.

9. Manage your inbox

- Handle each message as few times as possible.
- When you open it, determine whether it is official or transitory. Then decide if you will deal with it, delegate it, or delete it.

Adapted from the Government Records Service Guide: Email Tips

EMAIL RECORDKEEPING RESPONSIBILITIES

Do government records management rules apply to email? Yes they do! Emails are records of the work we do, and the management and retention of email must comply with approved information schedules (ARCS and ORCS). Employees need to create and keep sufficient records to document work activities and decisions.

It is important to ensure that significant business emails are:

1. **Filed** in the office recordkeeping system (e.g., paper file folders, shared drives, Commission systems).
2. **Managed** (classified, retained and disposed) in accordance with approved information schedules.
3. **Accessible** to authorized staff and available in response to Freedom of Information (FOI) and litigation requests.

Do I need to file every email?

No, you do not. Many emails are only of temporary usefulness and may be considered transitory. Transitory records are typically kept for short periods of time for: convenience or reference; preparation of revisions or a final version of a record; or, to complete immediate and minor transactions.

Transitory email examples include:

- Simple messages regarding **commonplace interactions** (e.g., request to return a call)
- **Drafts or revisions** that do not provide information on decisions or approvals not available elsewhere.
- **Copies** for reference purposes.
- **Duplicates** that have been filed or summarized in an official record
- Messages (e.g., telephone, email, text or instant messages) that **do not document** a decision, activity, or transaction, nor add information needed to meet financial, legal, audit, or statutory requirements.

Tip 1: For more examples, refer to the *Official vs Transitory Records* guide
Tip 2: For guidance on when to keep or destroy emails, refer to the *Email Decision Diagram – Keep or Destroy*?

Who is responsible for filing internal (within the Commission) email messages?

Usually the email sender is responsible for filing significant emails and attachments.

Who is responsible for filing incoming email from external sources?

You are. If you are the sole recipient of an external email, or, if there are several recipients and you are responsible for the subject matter, you are responsible for deciding if the email is an official records or not, and manage it accordingly.

Each of us is responsible for determining which emails are official records and require filing. Consider the following when making this decision:

- Is it a **personal** email? If so, delete it promptly.

- Is the email for **temporary** use? If yes, it does not need to be filed and may be disposed as a transitory record.
- Were you sent a **'cc'** (carbon copy) or **'bcc'** (blind carbon copy) copy of the message? In most cases, you can delete this copy once it is no longer required for business purposes.
- Was the email widely distributed? For example, Commission-wide updates are received by all staff. The initiating office (as the sender) is responsible for filing an official file copy as they are responsible for the subject or function. Recipients can then manage their copies as transitory.
- If, however, you are the **main or sole recipient** of a significant business email from an external source, or are the primary person responsible for the subject, then file it (with any attachments) in your recordkeeping system. Once filed, the original email may be treated as redundant and deleted from your Outlook.

Five Benefits of Well Managed Email

1. You and your co-workers have access to the records you need to do your jobs. Email is classified and filed in the official recordkeeping system, not left inaccessible and unmanaged in an individual's email folders.
2. Email and all related records are linked together. A complete file of a specific activity, case, or topic is maintained – something that isn't possible if records are scattered across various email accounts.
3. Email is disposed of in accordance with approved information schedules (e.g., ARCS, ORCS and the Transitory Schedule).
4. Email server space usage is reduced as duplicate and transitory emails are promptly deleted.
5. Authorized staff can locate all records required to comply with Freedom of Information (FOI) or litigation requests.

Finally, best practices for working groups, or project teams:

Working groups, or teams, should assign responsibility for managing the records of a project or for shared mailboxes. Often the project manager will be responsible for filing key decision documents and supporting material, or the lead / chair of a working group will maintain the official records of the group. Take 5 minutes to discuss with your team who will manage group emails so everyone is clear on their responsibilities. This will clear unnecessary duplication, and also ensure the important records are being kept.

Adapted from Government Records Service Guide: Email: Your Recordkeeping Responsibilities

GLOSSARY OF TERMS

This glossary provides definitions for common information management terms used within the BC government and Commission environment.

A

- **Active records** are records in current use, or that need to be maintained in office space close to users (if records exist in physical format).
- **Administrative records** are common to all offices and distinct from operational records. Administrative records support common organizational functions such as the management of facilities, property, finance, personnel, and information systems. These records are managed (classified and scheduled) in accordance with the government Administrative Records Classification System (ARCS).
- **Administrative Records Classification System (ARCS)** is the government-wide standard for classifying, filing, retrieving and disposition scheduling of administrative records.
- **Alienation of records** is the permanent transfer of records and all present and future rights to the records from the Crown provincial to another entity. Records may only be alienated from the Crown with the approval of the Chief Records Officer, by means of an approved records schedule, or under legislation that approves the transfer of government assets, including records.
- **Archival appraisal** is the process of determining the final disposition of records. Records having enduring value to government and society are appraised by a government archivist, and preserved and made accessible at the government archives. Archival appraisal in the BC government is part of the process of developing a records schedule. Archival appraisal focuses on the information content of the records and the context of their creation. It takes into consideration their value for current administrative, operational, legal and fiscal use, as well as long-term evidential and informational values.

C

- **Classification system** is a system for organizing records based upon function and subject, for the purpose of facilitating retrieval and filing.
- **Confidential records** contain information requiring protection against unauthorized access or disclosure. Records are classified as confidential based on a variety of requirements, including but not limited to policy or legislation. For example, the *Freedom of Information and Protection of Privacy Act* identifies exceptions to the disclosure of requested information. Examples of Commission confidential records include well data, where confidentiality periods apply as defined in the drilling and production regulations, and First Nation consultations and draft agreements.
- **Conversion** is the act of transferring recorded information from one physical medium or format to another, especially data from an obsolete format to a current format (migration).

D

- **Data** includes individual facts or values not significant to a business until analyzed and/or preserved as a record of the business' transactions and operations. Data is the raw material stored in a structured manner that, given context, becomes information.

- **Database** is a common type of electronic system, consisting of a number of structured "fields" where pieces of information are stored, and can be sorted, manipulated, and retrieved in different ways for a variety of purposes. Complex databases re-use information and then display and print it in any number of combinations with other information, thereby creating electronic records.
- **Digital (electronic) records** consist of information that is entered, created, manipulated and/or stored on digital media or storage devices, and includes: records that are born digital; digitized records (converted from non-digital format); unstructured data (e.g. documents); and structured data maintained within electronic systems.

- **Electronic Document and Records Management System (EDRMS)** is an integrated software system capable of managing both electronic and physical records in accordance with ARCS, ORCS or other approved retention schedules.
- **Executive records** include the administrative and operational records of the offices of ministers, deputy ministers, assistant deputy ministers, and equivalent positions. Executive Records are covered by a government-wide special records schedule (102906).

- **File** is a set of related documents treated as a unit, uniquely identified, arranged in a logical sequence, and classified and scheduled together. The file is the logical entity used to organize and manage records. It identifies a group of records that together provide evidence of a transaction, case, subject or other business matter. A file may consist of one or more volumes.
- **File list** is used to describe, locate and retrieve files. Unless otherwise stated in government policy, file lists are required for the storage and final disposition of government records and must include the following information for each file: classification number, file code, file title, date range, Office of Primary Responsibility (OPR) designation, retention period and final disposition.
- **Final disposition** is the action taken after records become inactive under an approved records schedule. Final disposition can be: (1) secure destruction that ensures complete obliteration of information, regardless of the records medium or format; (2) transfer of the records to the custody of the government archives; or (3) transfer of the records to agencies outside government (also known as alienation). Final disposition must take place in accordance with RIM policy and authorized procedures.
- **Full retention** is the decision by a government archivist to preserve a set of records in its entirety (and in an accessible format). Retention decisions are documented in a records schedule.
- **Function** includes all of the activities, operations, or procedures performed by an organization to accomplish its mandate or mission. In the BC government, functions represent the major responsibilities that are managed by a program area, branch, or agency in order to fulfil its goals.
- **Functional analysis** includes analysis and categorization of business activities into a hierarchical structure of functions, activities and transactions. It is used by the BC government in the process of records classification and records schedule development.

- **Government records** include any recorded information created or received by government offices in the course of business activity and maintained as evidence of those activities, regardless of format (i.e., digital or physical).

I

- **Inactive records** are no longer required for ongoing business. These are records that are ready for final disposition or, in other words, records for which the scheduled active and semi-active retention periods have lapsed.
- **Information management** is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.

L

- **Life cycle** refers to the life span of a record from its creation or receipt to its final disposition. Retention periods in records retention and disposition schedules are closely associated with certain life cycle stages. The active period involves creation/receipt, classification, scheduling, maintenance and use; the semi-active period involves the continuing maintenance, use and storage; and the inactive period indicates the expiry of primary values and the disposition of the records by destruction or transfer to the archives, where they will be described, preserved, and made accessible.

M

- **Migration** includes preserving the integrity of electronic records/data by transferring them across hardware and software configurations and across subsequent generations of computer technology. Migration is used to ensure continued access to information as systems or media become obsolete or degrade over time.

O

- **Official file copy** is a complete, final, and authorized version of a record. An official file copy is the version that is classified and filed in the office recordkeeping system.
- **Operational records** relate to those mandated functions which are unique to a government public body, for which it is responsible for performing according to statute, regulation or policy. These records are described in an Operational Records Classification System (ORCS).
- **Operational Records Classification System (ORCS)** is a records schedule that's tailored to the operational records of a specific program of government, in accordance with government-wide standards. ORCS facilitate the classification, filing, retrieval and disposition of operational records.

P

- **Personal information** is recorded information about an identifiable individual other than contact information, as defined in the *Freedom of Information and Protection of Privacy Act*.

Q

- **Quality control** includes procedural steps that ensure that scanned, imaged, converted, or migrated records, systems, and applications yield the same data and functionality as the source record from which they are reproduced. Quality control aims to establish the authenticity, accuracy, and usability of official file copies.

R

- **Records** include any recorded information created or received, and retained in the day to day operations of business. Includes "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise" as defined in the *Interpretation Act*.
- **Recordkeeping system** within an office refers to a shared ARCS/ORCS based filing system in which non-transitory records and created, protected, retained and destroyed in accordance with legal retention schedules.
- **Redundant source records** are records that have been copied or converted, where the copies, once verified to ensure their accuracy and authenticity, replace or supersede the originals and are filed in the office recordkeeping system.
- **Retention period** is the length of time a file is retained, as governed by the records schedule.
- **Retention schedule** is a timetable for maintaining an organization's records. It governs the life cycle of a file from creation, through active use within an office, through a record's move to inactive storage (when appropriate) to final destruction or their transfer to the custody and control of the Provincial Archives. The approved retention schedules for government records are defined in ARCS and ORCS and are applied throughout a records life cycle.

S

- **Selective retention** is the decision by a government archivist to preserve part of a set of records. Records schedules include specific retention criteria to help with identifying those records that need to be kept.
- **Semi-Active records** are used only occasionally and do not need to be maintained in the office space of the Commission. While they still have value, they can be stored in economical, offsite storage facilities.

T

- **Transitory records** are records of temporary usefulness that are not an integral part of an administrative or operational record series. Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions. As with all records, they can exist in any format or medium (paper or electronic). These records are not regularly filed with official Commission records within filing systems. They are only required for a limited period of time to complete a routine task or prepare an ongoing record.

Adapted from the Government Records Service RIM Glossary

MANAGING DRAFTS AND WORKING MATERIALS

Do I need to manage drafts and working materials in all formats?

YES. Drafts and working materials must be managed regardless of their format or media (i.e., digital or paper). The Commission uses approved information schedules (*ARCS* and *ORCS)* to govern how official records are managed, and we all need to create and keep complete and accurate records sufficient to document our decision-making and work activities. When managing drafts and working materials, you will need to determine what to keep (what is relevant to form a complete file), and what may be considered transitory, and destroyed.

Tip 1: When working on a document with others, it's good to designate one person to be responsible for filing the official copy of the final version as well as relevant working materials.

Tip 2: See the *Document Naming Conventions* guide for ideas on how to manage versions/drafts of documents.

Can I destroy all drafts and working materials as "transitory" records?

NO. Relevant drafts and working materials are treated as official records and cannot be destroyed as transitory. Relevant drafts and working materials contain significant notes, comments, approvals and substantial changes, and may relate to the following:

- Working materials relating to the preparation of legislation, Treasury Board or Cabinet submissions
- Any developmental drafts that, in your judgment, reflect important milestones
- Working materials necessary to understanding final document
- Operational records covered by the Commission's *Operational Records Classification System* (*ORCS*)

Such records are required for statutory, legal, fiscal, administrative or operational purposes, and need to be retained in your office recordkeeping system.

For a record to be deemed "transitory", it must not be required to meet statutory obligations or to sustain administrative or operational functions. Transitory records are records of temporary usefulness. They are only required for a limited period of time to complete a routine action or prepare a record, such as notes which are transcribed into the next draft. They are not important to a record series, and are not filed within official Commission files or electronic systems.

Tip 3: See the *Official vs. Transitory Records Quick Reference Guide* for more information on transitory records

Adapted from the Government Records Service Guide: Managing Drafts and Working Materials

QUICK REFERENCE GUIDE: "OFFICIAL" vs "TRANSITORY" RECORDS

What is a Record? A record includes all recorded information and is considered to be either "official" or "transitory". It is the information we use and access daily through a variety of sources, such as email, documents, databases, intranets, social media and the internet. Records can include "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise" (*Interpretation Act*).

OFFICIAL Records Must Be Kept & Filed

Official Records:

- Document or support the delivery of Commission programs
- Document Commission business or support its organization, policies, procedures, transactions or operations
- Show evidence of decision-making or courses of action taken
- Include information that must be held by the Commission by law
- Includes information created or received by the Commission and having long-term archival value

Official records may be required for financial, legal, audit, operational or statutory purposes and **need to be managed according to approved retention and disposition schedules** (*Administrative* and/or *Operational Records Classification Systems*).

- Business unit activities documentation (e.g., calendars, work plans)
- Information that supports the history or development of a decision, project or relationship
- Documentation that provides evidence of a significant action (e.g., change of scope or direction, verification or approval to proceed)
- Draft documents (or revisions) that reveal key decisions or approvals, substantive changes, or recommendations for taking a different course of action
- Final reports, plans or studies
- Policies, procedures, instructions or directives
- Drafts and working materials relating to the preparation of Treasury Board and Cabinet submissions
- Drafts and working materials relating to the preparation of legislation
- Meeting agendas and minutes (if you are the staff member responsible for the meeting or representing the Commission)
- Records about advice or recommendations
- Documentation relating to a compliance matter, or how a case was managed
- Documentation supporting the initiation/planning, authorization, or completion of business transactions
- Formal communications about official business (can include emails, voicemail, or text messages)

TRANSITORY Records Can Be Destroyed

Transitory Records:

- Are of **temporary** usefulness and only needed for a limited period of time to complete a routine action or to prepare a final record
- Do not document Commission business
- Are not required to meet statutory obligations or sustain administrative or operational functions

Transitory records should not be included in your office's recordkeeping system. **You can dispose of transitory information as soon as you are finished with it.**

- Emails, voicemail, or text messages that are not required to document a decision, action or transaction (e.g., personal message, announcement of a social event, meeting arrangements, or an email conveying an attachment)
- Copies of records created for reference or convenience, and no longer needed (unless you are the staff member responsible for the matter)
- "Input" source documents that are no longer required
- Direct mail/email notices and bulletins
- Course or conference announcements
- Working files (e.g., rough notes, calculations, outlines, lists of ideas)
- Drafts or revisions that do not provide information on key decisions or approvals, or that can be found elsewhere
- Routine correspondence about drafts or revisions
- External company profiles, pamphlets or catalogues (general information)
- Free trial CDs and DVDs
- Blank forms, including blank e-forms and e-templates, or out-of-date stationary
- Out-of-date published material (e.g., pamphlets, brochures or newsletters)

WHAT IS AN OFFICE RECORDKEEPING SYSTEM?

Employees need to create and keep complete and accurate records to document their decision-making and work activities. This applies to all types of Commission records, especially documents which provide the best evidence of Commission business activities, transactions, policy or decisions. These records must be managed in accordance with government policy and standards, which require managing Commission records in a recordkeeping system.

An office recordkeeping system is designed to hold, protect, retain and dispose of records in accordance with approved retention schedules. Per legislation, we must abide by administrative and operational retention schedules (ARCS and ORCS-based filing systems) to manage our records.

Types of office recordkeeping systems:

- **Hardcopy (Paper) Records:** Printing and filing records into a filing system (such as our Fort St. John file room) can be a suitable approach for some types of records, but is not viable for many categories of records. It is also not consistent with key government goals of electronic operations, reduced carbon emissions, and enhanced information sharing.

- **Shared Drives**: These can be organized and administered in accordance with ARCS and ORCS. This method is viable for limited volumes and types of electronic records, and is suitable as an interim approach pending use of a fully-functional recordkeeping system (i.e., EDRMS).

- **Electronic Document and Records Management System (EDRMS):** A comprehensive recordkeeping system with a full range of records management tools. It includes a records classification structure with linked retention schedules (ARCS and ORCS), and sophisticated searching and retrieval functions. EDRMS enables integrated management of both paper and electronic records and is the approved government standard. *This is the recordkeeping system the Commission is actively working towards.*

Our Commission office recordkeeping system covers a few places!
The file room in Fort St John holds paper files, systems such as AMS hold "official" electronic records, and we hold documents in our corporate shared drives.

A key component of a recordkeeping system is using ARCS and ORCS. ARCS and ORCS combine a records classification system with retention and disposition schedules for government records. What does this mean?

- A **classification system** identifies and describes the records created or received by offices.
- A **records retention and disposition schedule** is the timetable outlining the life span of a record from creation, through active use within an office and temporary retention in offsite storage (for paper files), to final destruction or transfer to the BC Government Archives.

Responsibilities in an office recordkeeping system:

- **Employees** are responsible for documenting their work by ensuring key records they create or receive are filed in their office recordkeeping system.
- **Program areas** are responsible for maintaining a shared office recordkeeping system that is organized and administered in accordance with government records legislation and policy.

Storing records in employee-specific network drives (F: drive) or email folders is not equivalent to filing them in the office recordkeeping or shared filing system. This creates **risks** such as:

- Restricted access – co-workers who require records do not have access to the drive and its contents
- Incomplete records – key records may not be classified and filed
- Difficulty searching – records may be missed when responding to requests made under the Freedom of Information and Protection of Privacy Act (FOIPPA) or during the legal document discovery process

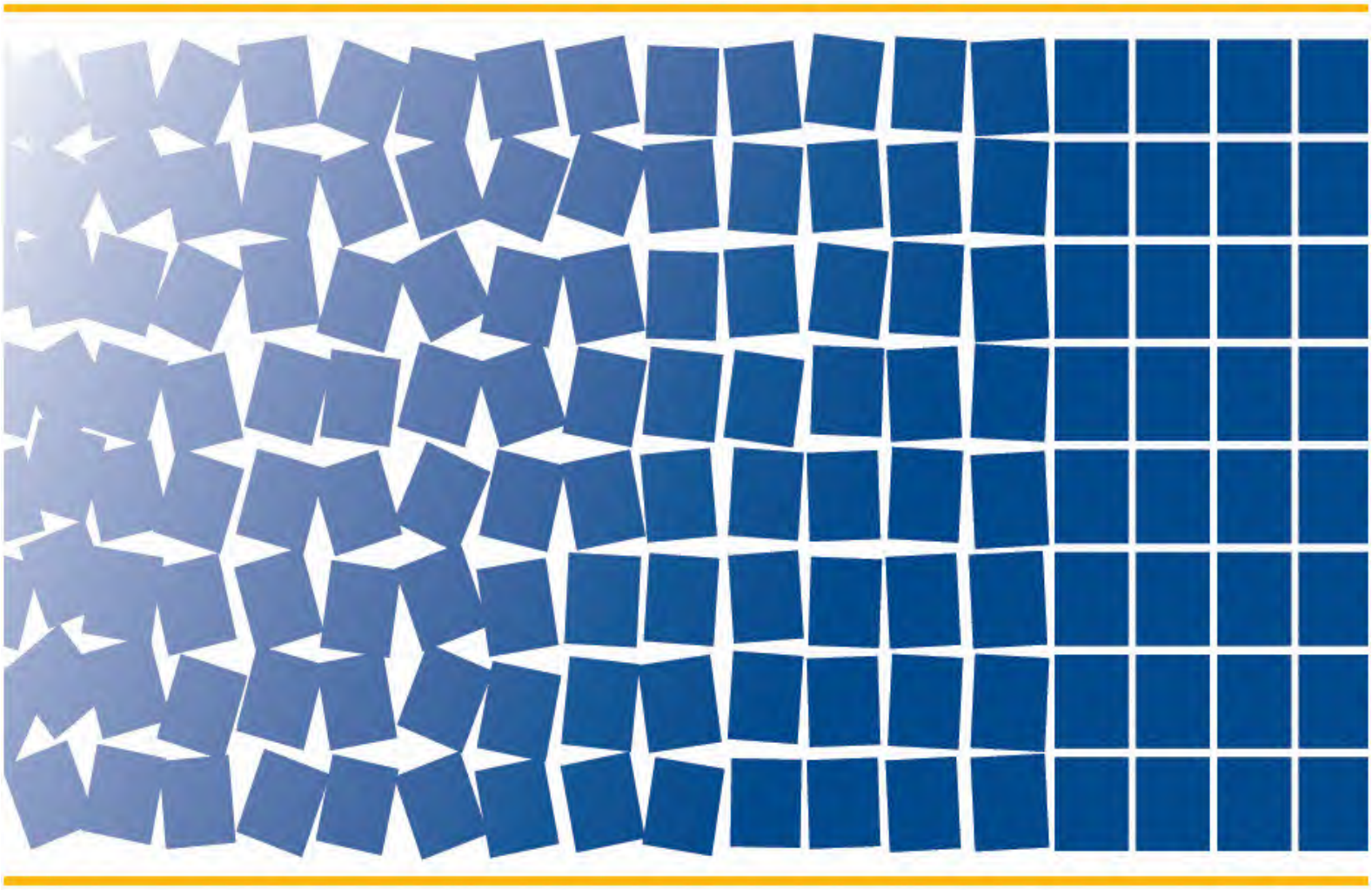
Government's requirements for managing records:

In the BC government, the requirements for establishing office recordkeeping systems are set in the following legislation, policy and standards:

- *Information Management Act*
- *Freedom of Information and Protection of Privacy Act*
- *Core Policy and Procedures Manual Chapter 12*
- *Administrative* and *Operational Records Classification Systems* (*ARCS* and *ORCS*)

Adapted from Government Records Service Guide: Office Recordkeeping System

HUMAN RESOURCES ARCS SUPPLEMENT ADMINISTRATIVE RECORDS CLASSIFICATION SYSTEM



BRITISH COLUMBIA

GOVERNMENT RECORDS SERVICE

HUMAN RESOURCES ARCS SUPPLEMENT

ADMINISTRATIVE RECORDS CLASSIFICATION SYSTEM

BRITISH COLUMBIA

GOVERNMENT RECORDS SERVICE

Shared ServicesBC

Schedule No: 206270
Amendment No (If applicable): 206270

RECORDS RETENTION AND DISPOSITION AUTHORITY

This is a recommendation to authorize an ongoing records schedule.

Title: Human Resources ARCS Supplement

Provincial agencies, boards and commissions covered by the *Document Disposal Act* (RSBC 1996, c. 99).

Description and Purpose:

The *Human Resources ARCS Supplement* establishes a classification system and retention and disposition schedule for human resources management and payroll services records created and received by British Columbia agencies, boards and commissions with their own internal human resources and payroll services.

In 2007, the retention periods in Section 5 of the *Administrative Records Classification System (ARCS)* were significantly reduced as a result of the government centralization of human resources management and payroll functions. The retention periods no longer meet the business needs of agencies that do not use the centralized government services.

These records document employee awards and recognition; benefits; charitable donations; job description and classification; employee work history; employer-employee relations; leave, payroll and time reporting; occupational safety, health and accidents; staffing projections and planning; staffing and recruitment; and training and development.

For more information, see the attached schedule.

Start Date: 1871/01/01 - ongoing

Recommended retention and disposition: scheduled in accord with attached records schedule.

THE UNDERSIGNED ENDORSE THE RECOMMENDATIONS:

M. Lauzon Records Officer signature Print Name: Mike Lauzon	2014/01/21 Date
W Boyd ADM or Executive Director signature Print Name:	2014/01/22 Date
J. Ahmed Deputy Minister or Corporate Executive signature Print Name: SARF AHMED	2014/03/12 Date

THE PUBLIC DOCUMENTS COMMITTEE CONCURS:

Chair, PDC signature Print Name:	April 3, 2014 Date

THE SELECT STANDING COMMITTEE ON PUBLIC ACCOUNTS APPROVES THE RECOMMENDATION OF THE PUBLIC DOCUMENTS COMMITTEE:

April 9, 2014
Date

APPROVED BY RESOLUTION OF THE LEGISLATIVE ASSEMBLY:

April 10, 2014
Date

Redacted

Shared ServicesBC

Schedule No: 206270
Amendment No (If applicable): 206270

RECORDS MANAGEMENT APPRAISAL:
This appraisal documents the recommendation for active and semi-active retention periods.

These records are created and received under the authority of the enabling acts of each agency, board or commission covered by the *Document Disposal Act* and subsequent legislation governing the responsibilities and functions of those bodies.

Under this *ARCS* supplement, agencies, boards and commissions will be authorized to apply the schedule to human resources and payroll management records for which the retention periods and final dispositions meet government's information requirements, ensure fiscal and audit control and protect government's legal rights and liabilities, and provide for effective management of the agency's functions. Upon approval of this *ARCS* supplement, and before applying it to their records, each agency will submit a list of the classifications that do not apply to their records.

Agencies, boards and commissions may in future submit a revised *ARCS* supplement to meet individual retention and disposition requirements, which will be subject to the same reviews and approvals as other administrative or operational records classification systems.

M. Lauzon	2014/01/21
Client Service Specialist, Broader Public Sector signature **Print Name: Mike Lauzon**	**Date**

ARCHIVAL APPRAISAL:
This appraisal documents the recommendation for final disposition.

The final disposition recommendations protect records considered to have significant evidential and historical values. The specific reasons for retaining certain records are stated within the *ARCS Supplement*, as well as in the Executive Summary.

Record series or groups of records which will be retained in their entirety are indicated by "Full Retention."

Record series or groups of records which will be retained in part are indicated by "Selective Retention." Selective retention means that portions of the record series will be retained by means of recognized archival selection criteria. For the meaning of selective retention with respect to a specific record series, see the attached schedule.

The definitions of both selective and full retention provide that records will be preserved in the government archives, and that unnecessary duplicates, transitory materials, and ephemera may be discarded.

	2014/01/21
Senior Archivist signature **Print Name: Mary McIntosh**	**Date**
The undersigned endorses the appraisal recommendations: Glen Isaac	2014/01/21
Manager, Infrastructure and Strategy signature **Government Records Service, Information Access Operations** **Print Name: Glen Isaac**	**Date**

Request for Records 2021-00140

A SA FD

HUMAN RESOURCES ARCS SUPPLEMENT (HRAS)

EXECUTIVE SUMMARY

The *Human Resources ARCS Supplement (HRAS)* establishes a classification system and retention and disposition schedule for the administrative functions and activities that are unique to those agencies with their own internal human resources and payroll services.

In 2007, the retention periods in *ARCS Section 5 Human Resources Management* were significantly reduced as a result of government centralization of the human resources management function. The records retention periods no longer met the business requirements of agencies with their own internal human resources and payroll services.

These records document human resources activities performed by agencies with their own internal human resources and payroll services, including: awards and recognition; benefits; charitable donations; job description and classification; employee work history; employer-employee relations; leave, payroll and time reporting; occupational safety, health and accidents; staffing projections and planning; staffing, recruitment and competitions; and training and development.

HRAS establishes a classification system and retention and disposition schedule for human resources records created and received by British Columbia agencies under the *Public Service Act* (RSBC 1996, c. 385), *Workers Compensation Act* (RSBC 1996, c. 492, part 3), and *Occupational Health and Safety Regulation* (BC Reg. 296/97).

The active and semi-active retention periods specified in the schedule meet all administrative, legal, fiscal, and audit requirements. The final dispositions have been reviewed to ensure that records having enduring evidential and historical values are preserved.

The following summary describes secondaries that were affected by the human resources and payroll centralization accompanied with revised retention schedules and final dispositions. Please consult *HRAS* for further information.

1) Policy and procedures
(secondary -00 throughout *HRAS*) — SO 5y FR

Throughout *HRAS,* the government archives will fully retain final versions of all policies, procedures, standards and guidelines created by offices having primary responsibility for their development and approval. These records have significant evidential value for documenting the functions covered by *HRAS.*

2) Salary schedules — SO 7y FR
(secondary 7360-05)

These records document employee compensation.

		A	SA	FD
	FR = The government archives will fully retain salary schedules because they provide a concise history of salary rates and rate increases over time. These records document salary ranges, rates and increases for bargaining unit and excluded positions.			
3)	Strike and essential service planning case files (secondary 7480-45)	SO	nil	FR
	These records document strike contingency planning and the determination of essential service levels in the event of job action. SO = upon conclusion of strike, and when no longer required for reference purposes FR = The government archives will fully retain strike and essential service planning files because they significantly document the employer's plans and strategies for responding to strikes by its unions.			
4)	Collective agreements and memoranda of agreement (secondary 7480-02)	SO	nil	FR
	These records document the agreed upon terms and conditions of employment for bargaining unit employees. SO = upon termination of agreement and expiry of the two-year limitation period under the *Limitation Act* (SBC 2012, c.13), and when no longer required for reference purposes FR = The government archives will fully retain collective agreements and memoranda of agreement because they provide a history of the terms and conditions of employment for bargaining unit employees.			
5)	Collective bargaining negotiations and preparation case files (secondary 7480-25)	SO	nil	FR
	These records document collective bargaining negotiations and the agreed upon terms and conditions of employment for bargaining unit employees. SO = upon conclusion of negotiations and, if relevant upon expiry of agreement and the two-year limitation period under the *Limitation Act* (SBC 2012, c.13), and when no longer required for reference purposes. FR = The government archives will fully retain the collective bargaining negotiations and preparation case files because they document the positions of the employer and its unions during the collective bargaining process.			

		A	SA	FD
6)	Position history files (secondary 7360-25)	SO	10y	DE

These records include job descriptions, organization charts, classification authorization documents, classification decision rationale, position exclusion agreements, on-site interview notes, work examples received from incumbent employees and their supervisors, comparative job descriptions and corresponding rationale, and classification appeal decisions.

SO = when the position is redundant

10y = The ten-year retention period provides sufficient time for research, consultation and potential reactivation of closed files. However, after a lapse of 10 years, it is unlikely that the position will be recreated or the files will have any reference value.

7)	Employee personnel files (secondary 7385-20)	SO	10y	DE

These records document the employment history of agency employees. At a minimum, a file contains a copy of their application and/or résumé, a copy of their offer/confirmation letter, OICs for executive and non-executive appointments, personal and emergency contact information, copies of any documents that will confirm job qualifications (e.g., degrees and licences) and which have been verified for authenticity, the oath of employment signed by the employee and a commissioner for taking affidavits for BC, a signed standard of conduct acknowledgement, and a signed internet Communications Technology Usage Agreement.

SO = upon retirement, resignation, or employment termination

10y = The ten-year semi-active retention period provides a reasonable length of time for consultation and reactivation of the files if the employee is again employed. It is consistent with the retention period within the *Public Service Personnel Management ORCS*, schedule 181080.

8)	Employee pay files (secondary 7550-20)	SO	7y	DE

These records document hiring notices, reclassifications, personal tax credit returns, direct deposit forms, timesheets, leave forms, temporary appointments, pension termination notices, checklists, and salary adjustment worksheets.

SO = upon retirement, resignation, or employment termination

7y = The seven-year retention period ensures that employee pay, work schedule, and leave information, not captured electronically, is retained

for two years after employment termination, as required under the *Employment Standards Act* (RSBC 1996, c. 113, s. 28). It also ensures that the records are retained for five years allowed for purchasing pensionable service and are available to taxation authorities which have the right under the Income Tax Act (RSC 1985, c. 1-5, ss. 230(4) and 231.1) to investigate income tax returns filed for the previous six years.

9) All Other Records DE

All other records are destroyed at the end of their semi-active retention periods. The retention of these records varies depending on the nature of the records and the function performed, but does not exceed seven years. Any information from these records that has ongoing value is adequately documented under secondaries with longer retentions and/or full or selective retention appraisals within *HRAS* or in *ARCS*, such as summary reports, policy records, executive briefing notes (*ARCS* secondary 280-20), and annual service plan reports (*ARCS* secondary 400-02). These records have no enduring value to government at the end of their scheduled retention periods.

END OF EXECUTIVE SUMMARY

HUMAN RESOURCES ARCS SUPPLEMENT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

TABLE OF CONTENTS

INTRODUCTION

SECTION 1 7300 -7999 HUMAN RESOURCES ARCS SUPPLEMENT

INDEX

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

INTRODUCTION TO THE *HUMAN RESOURCES ARCS SUPPLEMENT*

For further information, contact your Records Officer.

Request BCER2024-001 - Page 98 of 249

1. General

This introduction provides an overview of the functions and activities documented in records classified and scheduled under the Human Resources ARCS Supplement (*HRAS*).

For general information about the purpose, organization, and elements of *ORCS* in general, and of the *Administrative Records Classification System* (*ARCS*), see the *ARCS and ORCS User Guide* available on BC Government's Records Management web site at http://www.gov.bc.ca/citz/iao/arcs/admin/arcs_orcs_user_guide.pdf. It is designed to help you understand, interpret and use *ARCS* and *ORCS*.

For special schedules that cover records that are not covered by *ARCS* and *ORCS*, see http://www.lcs.gov.bc.ca/cimb/special/default.asp.

For legislation, policies, and standards for managing records in the BC Government, see http://www.gov.bc.ca/citz/iao/records_mgmt/policy_standards/.

For tips, guides, and FAQs on related topics, see http://www.gov.bc.ca/citz/iao/records_mgmt/guides/.

For Records Officer contact information, see http://www.gov.bc.ca/citz/iao/records_mgmt/rec_officers/.

2. Overview of *HRAS* Purpose and Structure

The administrative records covered by this *HRAS* relate to the operations and services your ministry or agency provides in accordance with statute, mandate, and/or policy.

HRAS has the following parts:

- Executive Summary:
  - a copy of the signed records retention and disposal authority (ARS 008) form
  - a high-level overview of *HRAS*
- Table of Contents
- Introduction (this section)[1]
- Section 1 and any other numbered sections with classifications and schedules for the records covered by *HRAS*; see part 3 below for further information
- Index

[1] Pre-2011 *ORCS* have "How to Use" sections instead of the Introduction. Much of the information that used to be provided in the How to Use section is now available in the *ARCS/ORCS User Guide* available on the Records Management web site.

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

ORCS KEY: the Key to your *ORCS* Codes and Acronyms

The following codes and acronyms are used throughout this *ORCS*:

Office information:	**OPR** = Office of Primary Responsibility
Records life cycle:	**A** = Active **SA** = Semi-active **FD** = Final Disposition
Active and semi-active periods:	**CY** = Calendar Year **FY** = Fiscal Year **NA** = Not Applicable **SO** = Superseded or Obsolete **w** = week **m** = month **y** = year
Final dispositions:	**DE** = Destruction **FR** = Full Retention **SR** = Selective Retention **OD** = Other Disposition
Special flags:	**FOI** = Freedom of Information/Privacy **PIB** = Personal Information Bank **VR** = Vital Records

For further explanation of terms, see the *ARCS and ORCS User Guide*.

3. The Functions and Activities Covered by this *ORCS*

Section Number	Primary Numbers	Section Title
Section 1	7300-7999	Human Resources ARCS Supplement

Covers records relating to human resources (HR) activities performed by agencies that have their own internal HR services. This includes records relating to: awards and recognition; benefits; charitable donations; job description and classification; employee work history; employer-employee relations; leave, payroll and time reporting; occupational safety, health and accidents; staffing projections and planning; staffing, recruitment and competitions; and, training and development.

4. Legal Authority of *HRAS*

Under provisions of the *Document Disposal Act* (RSBC 1996, c. 99), *HRAS* has been reviewed and endorsed by the following authorities:

- government archivists
- your executive
- the Public Documents Committee
- the Select Standing Committee on Public Accounts

Upon approval by the Legislative Assembly, *HRAS* has statutory authority governing the retention and disposition of the records that it covers.

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

SECTION 1

HUMAN RESOURCES ARCS SUPPLEMENT

PRIMARY NUMBERS

7300 – 7999

Section 1 covers records relating to human resources (HR) activities performed by agencies that have their own internal HR services. This includes records relating to: awards and recognition; benefits; charitable donations; job description and classification; employee work history; employer-employee relations; leave, payroll and time reporting; occupational safety, health and accidents; staffing projections and planning; staffing, recruitment and competitions; and, training and development.

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

SECTION 1 TABLE OF CONTENTS

HUMAN RESOURCES ARCS SUPPLEMENT

7300 - 7999

7300 HUMAN RESOURCES ARCS SUPPLEMENT – GENERAL

7310 AWARDS AND RECOGNITION

7315 BENEFITS

7320 CHARITABLE DONATIONS

7360 JOB DESCRIPTION AND CLASSIFICATION

7385 EMPLOYEE WORK HISTORY

7480 EMPLOYER-EMPLOYEE RELATIONS

7550 LEAVE, PAYROLL AND TIME REPORTING

7560 OCCUPATIONAL SAFETY, HEALTH AND ACCIDENTS

7580 STAFFING PROJECTIONS AND PLANNING

7665 STAFFING, RECRUITMENT AND COMPETITIONS

7730 TRAINING AND DEVELOPMENT

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7300 HUMAN RESOURCES ARCS SUPPLEMENT - GENERAL

Records not shown elsewhere in the *Human Resources ARCS Supplement* that relate generally to human resources activities performed by agencies that have their own internal human resources services.

This primary also covers records relating to the development of human resources policy.

Record types include correspondence and reports.

NOTE Only records that cannot be classified in a more specific primary or secondary may be classified under this primary.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-00	**Policy and procedures** (covers final/approved versions of policies, procedures, standards, and guidelines pertaining to this section) FR: Throughout this section, the government archives will fully retain all policy and procedure files created by offices having primary responsibility for policy and procedure development and approval. These records have evidential value.	SO	5y	FR
-01	**General** NOTE: Throughout this section, this secondary covers miscellaneous records that relate to the primary but do not document decisions and actions, and do not relate to topics that warrant specific classifications.	CY+1y	nil	DE
-06	**Human resources topical files** (arrange by subject [e.g., human rights, employment equity, job enhancement, and women's issues])	SO	nil	DE
-20	**Human resources policy development files** (arrange by policy) SO: when the policy is reviewed, developed, abandoned, or cancelled	SO	5y	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7310 AWARDS AND RECOGNITION

Records relating to the administration and management of programs that award and recognize employee contributions to improvements in service, operations, and the work environment.

Record types include correspondence, applications, evaluation and approval forms, and reports.

For ceremony planning, see *ARCS* secondary 220-20.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

			A	SA	FD
	All non-OPR offices will retain these records for:		SO	nil	DE
	-00	**Policy and procedures**	SO	5y	FR
	-01	**General**	CY+1y	nil	DE
	-05	**Award and recognition program information files** (arrange by program if volume warrants)	SO	nil	DE
PIB	**-50**	**Award and recognition applicant/recipient files** (arrange by program and/or employee, if volume warrants) SO: when decision is rendered, and if relevant, upon conclusion of appeal periods and appeals	SO+1y	nil	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7315 BENEFITS

Records relating to the administration and management of employee benefit packages (e.g., health and disability benefits, employment insurance, workers' compensation, life insurance, retirement and pension benefits, employee and family counseling services, salary and retirement savings plans).

Records types include correspondence, inquiries, manuals, reports and resolutions.

For benefit premium payments, see *ARCS* secondary 925-20.
For benefits accounting, see *ARCS* secondary 920-20.
For the tendering process and negotiation of contracts with plan carriers, see *ARCS* secondary 1070-20.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

			A	SA	FD
	All non-OPR offices will retain these records for:		SO	nil	DE
	-00	**Policy and procedures**	SO	5y	FR
	-01	**General**	CY+1y	nil	DE
	-05	**Benefit plan information files** (covers general information about each benefit plan) (arrange by specific benefit [e.g., life insurance, medical, and pension] if volume warrants)	SO	nil	DE
	-20	**Benefit administration files** (arrange by carrier and benefit type) (covers inquiries and resolutions, problems and issues involving participating employers, as well as researcher and analysis of various provisions of the plans) 8y: The eight-year retention period provides sufficient time for consultation.	FY+1y	6y	DE
PIB	**-25**	**Disability case management files** (arrange by employee surname) SO: when case is closed (i.e., employee requalifies for the Short Term Illness and Injury Plan (STIIP) or Long Term Disability (LTD) benefits by clearing the successive disabilities timeframe specified in the *LTD*	SO (cont'd)	20y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7315 BENEFITS

			A	SA	FD
-25	**Disability case management files (continued)**		SO	20y	DE
	SO:	*Plan Regulation* (BC Reg. 409/97, s.2.7) and outstanding issues [return to work, grievance, or arbitration] are concluded)			
	20y:	The 20-year retention period provides sufficient time for consultation and reactivation of the files if the employee is again on STIIP, LTD, Weekly Indemnity, or workers' compensation benefits.			

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7320 CHARITABLE DONATIONS

Records relating to facilitating employee charitable donations through payroll deductions. This includes planning and organizing annual fundraising campaigns, ensuring gaming fundraising events comply with the gaming license received from the provincial gaming branch, disbursing contributions to charities, and liaising with volunteer committees.

Record types include correspondence, forms, reports, financial records, and other types of records as indicated under relevant secondaries.

For audits, see *ARCS* primary 975.
For cheques and bank deposits, see *ARCS* primary 1050.
For committees, see *ARCS* secondary 200-20.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-02	**Campaign planning**	CY+2y	nil	DE
-04	**Donation reconciliation and disbursement records**	FY+1y	6y	DE

8y: The eight-year retention period is based on the six-year assessment period under the *Income Tax Act* (RSC 1985, c.1-5, s. 230(4)), and is consistent with the retention period for related financial records classified in *ARCS*.

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7360 JOB DESCRIPTION AND CLASSIFICATION

Records relating to the preparation of job descriptions, position classification and reclassification, salary schedules, bonus programs, incentive pay, and classification appeals.

Supervisors are responsible for defining their employees' duties, competencies and responsibilities in job descriptions (or job profiles) and submitting approved job descriptions for classification to the agency's internal human resources department. Classification is the formal evaluation of the relative value of different jobs within an organization. The relative value determines the appropriate salary.

Record types include correspondence, job descriptions, job evaluation plans, benchmarks, appeal notices, salary schedules, merit allowances, and forms.

For agency organization, see *ARCS* primary 105.
For the delegation of classification authority, see *ARCS* primary 265.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

			A	SA	FD
	All non-OPR offices will retain these records for:		SO	nil	DE
	-00	**Policy and procedures**	SO	5y	FR
	-01	**General**	CY+1y	nil	DE
	-02	**Bonus and incentive pay programs** 7y: The retention period ensures that bonus and incentive pay programs are available for a sufficient period of time for program review and planning purposes.	SO	7y	DE
	-04	**Job classification files** (covers job evaluation plans and benchmarks)	SO	nil	DE
	-05	**Salary schedules** FR: The government archives will fully retain salary schedules because they provide a concise history of salary rates and rate increases over time. These records document salary ranges, rates and increases for bargaining unit and excluded positions.	SO	7y	FR
PIB	**-20**	**Classification and review appeal files** (arrange by appellant or by job title for groups) SO: upon conclusion of the appeal and appeal periods	SO	10y	DE

(cont'd)

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7360 JOB DESCRIPTION AND CLASSIFICATION

			A	SA	FD
PIB	**-20**	**Classification and review appeal files** (continued)	SO	10y	DE
		10y: The 10-year retention period is based on the need to refer back to similar appeals when making a decision.			
		NOTE: The appeal decisions are also filed on the position history file sunder secondary -25.			
	-25	**Position history files** (arrange by position)	SO	10y	DE
		SO: when the position is redundant			
		10y: The 10-year retention period provides sufficient time for research, consultation and potential reactivation of closed files. However, after a lapse of 10 years, it is unlikely that the position will be recreated or the files will have any reference value.			
		NOTE: These files include job descriptions, organization charts, classification authorization documents, classification decision rationale, position exclusion agreements, on-site review notes, work examples received from incumbent employees and their supervisors, comparative job descriptions and corresponding rationale, and classification appeal decisions.			

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7385 EMPLOYEE WORK HISTORY

Records relating to the work history of all regular, part-time seasonal, auxiliary, and excluded employees.

Record types include correspondence, applications, forms, résumés, orders in council (OICs), copies of decrees, employee performance plans and reviews, agreements, reports, and photographs.

For article 29 committees, see *ARCS* secondary 200-20.
For complaints, disputes, and grievances, see secondary 7480-30.
For criminal record check consent forms (not hired), see secondary 7665-04.
For disability case management, see secondary 7315-25.
For training course development and delivery, see primary 7730.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

			A	SA	FD
	All non-OPR offices will retain these records for:		SO	nil	DE
	-00	**Policy and procedures**	SO	5y	FR
	-01	**General**	CY+1y	nil	DE
PIB	**-20**	**Employee personnel files** (arrange by surname) SO: upon retirement, resignation, or employment termination 10y: The 10-year semi-active retention period provides a reasonable length of time for consultation and reactivation of the files if the employee is again employed. It is consistent with the retention period within the *Public Service Personnel Management ORCS*, Schedule 181080. NOTE: At a minimum, an employee's personnel file may contain: a copy of their application and/or résumé, a copy of their offer/confirmation letter, OICs for executive and non-executive appointments, personal and emergency contact information, copies of any documents that will confirm job qualifications (e.g., degrees and licenses) and which have been verified for authenticity, the oath of employment signed by the employee and a commissioner for taking affidavits for BC, a signed standard of conduct acknowledgement,	SO (cont'd)	10y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7385 EMPLOYEE WORK HISTORY

			A	SA	FD
PIB	**-20**	**Employee personnel files** (continued)	SO	10y	DE

NOTE: and a signed internet Communications Technology Usage Agreement.

An employee's personnel file may also contain: police and criminal record check consent forms and clearances, formal performance evaluations, formal letters of commendation, employee data activity [EDA] reports, copies of social insurance cards, signed temporary assignment agreements, Canadian work visas or equivalent documentation, requests to process pay increases for managers, seniority reports/summaries, letters of resignation, separation reports, Early Retirement Incentive Program (ERIP) and Voluntary Departure Program (VDP) forms, deferred leave application forms, rehabilitative employment letters, paid absence prior to retirement forms, letters of suspension, discipline records and employees' requests for their removal, and letters advising employees of pay classification changes, assignments and reassignments, in/out of public service transfers, and retroactive classification.

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7480 EMPLOYER-EMPLOYEE RELATIONS

Records relating to employer-employee relations. This includes strike contingency planning, the determination of essential service levels in the event of job action, and the resolution of disputes, complaints, and misunderstandings with employees, including those that are subject to the grievance procedures in the collective agreement or covered by policy directives (e.g., the dispute resolution process for excluded employees, discrimination and personal and sexual harassment complaints) and employee engagement activities.

Record types include correspondence, forms, reports and plans.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-02	**Collective agreements and memoranda of agreement** SO: upon termination of agreement and expiry of the two-year limitation period under the *Limitation Act* (SBC 2012, c.13), and when no longer required for reference purposes FR: The government archives will fully retain collective agreements and memoranda of agreement because they provide a history of the terms and conditions of employment for bargaining unit employees.	SO	nil	FR
-20	**Collective agreement interpretation case files** (arrange by article number) (covers the employers' unilateral interpretation of the collective agreement)	SO	nil	DE
-25	**Collective bargaining negotiations and preparation case files** SO: upon conclusion of negotiations and, if relevant upon expiry of agreement and the two-year limitation period under the *Limitation Act* (SBC 2012, c.13), and when no longer required for reference purposes. FR: The government archives will fully retain the collective bargaining negotiations and preparation files because they document the positions of the employer and its	SO	nil	FR

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7480 EMPLOYER-EMPLOYEE RELATIONS

			A	SA	FD
	-25	**Collective bargaining negotiations and preparation case files** (continued) unions during the collective bargaining process.	SO	nil	FR
PIB	**-30**	**Dispute/complaint resolution files** (arrange by surname) SO: upon resolution of dispute or complaint, when decision is rendered and if relevant, upon conclusion of appeal periods and appeals 10y: The ten-year semi-active retention period provides a reasonable length of time for consultation.	SO	10y	DE
	-35	**Employee engagement activity files** (arrange by activity) SO: upon conclusion of activity	SO	5y	DE
	-40	**Labour relations reference files** (arrange by topic) SO: when no longer required for reference purposes	SO	nil	DE
	-45	**Strike and essential service planning case files** (arrange by issue or subject, whichever is appropriate) SO: upon conclusion of strike, and when no longer required for reference purposes. FR: The government archives will fully retain strike and essential service planning files because they significantly document the employer's plans and strategies for responding to strikes by its unions.	SO	nil	FR

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7550 LEAVE, PAYROLL AND TIME REPORTING

Records relating to payroll processing, accounting and approving employee attendance.

Some agency employees report their time worked and leave taken on an automated time and leave reporting system. However, paper timesheets and leave forms may be used for employees with irregular work schedules (e.g., shift or on call workers) and electronic forms are used to approve employee additions to base pay after the payroll deadline.

Record types include correspondence, forms, registers, reports, and copies of timesheets and leave forms.

For recovery of salary dollars from employee transfers, see *ARCS* primary 1190. For write offs of uncollectible salary overpayments, see *ARCS* primary 935.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

			A	SA	FD
	All non-OPR offices will retain these records for:		SO	nil	DE
	-00	**Policy and procedures**	SO	5y	FR
	-01	**General**	CY+1y	nil	DE
	-02	**Canada Savings Bond documentation**	CY+1y	nil	DE
	-03	**CRA account reconciliation and required documents** (CRA = Canada Revenue Agency) (covers tracking of CRA transfers, manual cheques, RRSP and other deductions or contributions) 8y: The eight-year retention period is based on the six year assessment period under the *Income Tax Act* (RSC 1985, c. 1-5, s.230 [4]) and is consistent with retention periods for accounts payable and reconciliations in *ARCS*.	CY+2y	5y	DE
	-04	**Pay run batch control and review reports**	CY+2y	nil	DE
	-05	**Payroll balancing and accounting reports**	CY+2y	5y	DE
PIB	**-20**	**Employee pay files** (arrange by employee surname) SO: upon retirement, resignation, or employment termination	SO (cont'd)	7y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7550 LEAVE, PAYROLL AND TIME REPORTING

		A	SA	FD
-20	**Employee pay files** (continued)			
	7y: The seven-year retention period ensures that employee pay, work schedule and leave information are retained for the five years allowed for purchasing pensionable service and are available to taxation authorities which have the right under the *Income Tax Act* (RSC 1985, c.1-5, ss. 230(4) and 231.1) to investigate income tax returns files for the previous six years.			

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7560 OCCUPATIONAL SAFETY, HEALTH AND ACCIDENTS

Records relating to promoting safe and healthy workplaces, as well as treating, reporting and investigating accidents, injuries, and diseases that result directly from work duties pursuant to the *Workers Compensation Act* (RSBC 1996, c. 492, part 3) and *Occupational Health and Safety Regulation* (BC Reg. 296/97). This includes agency and local worksite occupational safety and health (OSH) program planning, ergonomic assessments, first aid needs assessments, hazardous materials testing, incident reporting, and safety inspections.

Record types include correspondence, forms, books, logs, reports, and other types of records as indicated under relevant secondaries.

For disposal of hazardous material, see *ARCS* primary 525.
For emergency plans and procedures, see *ARCS* primary 275.
For joint employer/union health and safety committee, see *ARCS* primary 200.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-03	**First aid needs assessment**	SO	nil	DE
	SO: when replaced by new assessment in accordance with *Occupational Health and Safety Regulation* (BC Reg. 296/97 s. 3.16).			
	NOTE: Pursuant to *Occupational Health and Safety Regulation* (BC Reg. 296/97 s. 3.16), risks and hazards must be identified in worksites "within 12 months after the previous assessment or review and whenever a significant change affecting the assessment occurs in the employer's operations".			
-04	**First aid treatment books and logs**	SO	7y	DE
	SO: upon conclusion of first aid care, and when book or log is closed.			
	7y: The seven-year retention period satisfies the minimum three-year retention period for first aid treatment records specified under the *Occupational*	(cont'd)		

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7560 OCCUPATIONAL SAFETY, HEALTH AND ACCIDENTS

		A	SA	FD
-04	**First aid treatment books and logs** (continued) *Health and Safety Regulation* (BC Reg. 296/97 s. 3.19) and is consistent with the retention period for the joint health and safety committee files classified under *ARCS* secondary 200-20. NOTE: These records document work-related incidents that result in first aid treatment. Serious injuries, including exposure to contaminants, are reported to WorkSafe BC (the Workers' Compensation Board of Britsh Columbia) on incident investigation reports classified under secondary -20.	SO	7y	DE
-05	**Hazardous material information** (covers material safety Data Sheets [MSDS]) SO: when replaced by new information NOTE: If controlled products are used in the workplace, a Workplace Hazardous Materials Information System (WHMIS) program must be established. *Occupational Health and Safety Regulation* (BC Reg. 296/97 part 5) requires that MSDSs be updated at least every three years and that WHMIS programs are reviewed at least annually.	SO	nil	DE
-06	**OSH inspection files** SO: upon conclusion of inspection, and if relevant, upon implementation of corrective measures 7y: The seven-year retention period is consistent with the retention period for the joint health and safety committee classified under *ARCS* 200-20. NOTE: This secondary covers inspections to ensure compliance with the *Occupational Health and Safety Regulation* (BC Reg. 296/97 part 3). NOTE: For administrative convenience, these records may be classified on the joint health and safety committee file under *ARCS* secondary 200-20, rather than under this secondary.	SO	7y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7560 OCCUPATIONAL SAFETY, HEALTH AND ACCIDENTS

			A	SA	FD
	-07	**OSH program information** NOTE: This secondary covers agency and local worksite OSH program information (e.g., roles and responsibilities and instructions).	SO	nil	DE
	-08	**Personal protective equipment information** SO: upon completion of next annual review NOTE: *Occupational Health and Safety Regulation* (BC Reg. 296/97 part 8) requires that personal protective equipment programs be reviewed annually and that equipment fit tests be repeated at least annually.	SO	nil	DE
PIB	**-09**	**Refusal to work because of unsafe conditions** (arrange by employee surname) SO: upon conclusion of investigation, and if relevant, upon implementation of corrective measures 7y: The seven-year retention period is consistent with the retention period for the OSH inspection files classified under secondary -06.	SO	7y	DE
PIB	**-20**	**Work-related incident reporting files** (arrange by employee surname) (covers accident and incident reports, employer's report of injury or occupational disease [WCB form 7], first aid report [WCB form 7A], and may include worker's report of injury or occupational disease to employer [WCB form 6a]) SO: upon adjudication of claim by WorkSafeBC, and if relevant, upon implementation of corrective measures 7y: The seven-year retention period is consistent with the retention period for the first aid treatment records classified under secondary -04. NOTE: These records document work-related incidents that result in death, time loss, or medical attention or have the potential of causing serious injury to a worker or involve a major structural failure or exposure to hazardous or bio-hazardous substances (e.g., asbestos and avian influenza viruses). These	SO (cont'd)	7y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7560 OCCUPATIONAL SAFETY, HEALTH AND ACCIDENTS

			A	SA	FD
PIB	**-20**	**Work-related incident reporting files** (continued) incidents must be reported to WorkSafeBC even if a claim is not anticipated.	SO	7y	DE
PIB	**-25**	**Employee health case files (no exposure)** (arrange by employee surname) (covers ergonomic assessments, hepatitis B vaccination records, musculoskeletal injury prevention client records, pre-placement assessment examinations and outcomes, and related health records) SO: upon resignation, employment termination, retirement or death while in service 10y: The retention period is consistent with the retention period for the related employee files and health-related absence files. The retention period also satisfies the minimum 10-year recommendation for the retention of vaccination records stated in WorkSafe BC's guidelines: G6:34-5 *Record keeping requirements.* NOTE: This secondary covers records that do not document exposure to latent biological hazards.	SO	10y	DE
PIB	**-30**	**Latent biological hazard exposure case files** SO: upon resignation, employment termination, retirement, or death while in service 30y: The retention period provides a reasonable length of time for the effects of the exposure to become apparent. NOTE: This secondary covers records that document exposures to latent biological hazards, the effects of which may occur years later (e.g., asbestos, blood borne pathogens, tuberculosis and radiation).	SO	30y	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7580 STAFFING, PROJECTIONS AND PLANNING

Records relating to agency staffing projections and planning, including staff reductions and surpluses resulting from workforce adjustment and voluntary exit programs.

Record types include correspondence, surveys, and reports.

For budget planning, see *ARCS* primary 1000.
For strategic planning, see *ARCS* secondary 400-20.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-02	**Seniority, recall, and vacancy lists** NOTE: Eligibility lists are classified under secondary 7665-20.	SO	nil	DE
-03	**Staffing requirements planning files** NOTE: This secondary includes FTE planning and utilization, staff requisitions, pre-retirement and succession planning, priority placements, and workforce adjustment and planning.	CY+1y	6y	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7665 STAFFING, RECRUITMENT AND COMPETITIONS

Records relating to the staffing of positions, including recruitment of employees and competitions for vacant positions.

Record types include correspondence, forms, reports, and other types of records as indicated under relevant secondaries.

For employee personnel files, see secondary 7385-20.
For job descriptions, see secondary 7360-25.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-03	**Model interview questions**	SO	nil	DE
-04	**Criminal record check consent forms (not hired)**	CY	5y	DE

6y: The retention period satisfies the five-year retention period required by the Royal Canadian Mounted Police (RCMP) Canadian Police Information Centre (CIPC) auditors for the retention of *Criminal Records Review Act* (RSBC 1996, c. 86) consent forms.

NOTE: This secondary covers unsuccessful applicants' consent forms for record checks under the *Criminal Records Review Act* and *Public Service Act Directive 3.6 Police Record Checks*. Consent forms of successful job applicants are filed on the relevant employee file (secondary 7385-20).

NOTE: As required by part D of *Public Service Act Directive 3.6 Police Record Checks*, agencies are required to destroy or return all police documentation to job applicants, including the results of police record checks, and eliminate all references that identify applicants with criminal records. Therefore, police record check consent forms should only indicate that a check has been undertaken.

-05	**Selection standards reference material**	SO	nil	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7665 STAFFING, RECRUITMENT AND COMPETITIONS

			A	SA	FD
	-06	**Student recruitment/selection information** NOTE: This secondary includes co-op, articling, intern and summer student recruitment information. When students are hired, their employment records are classified under 7385-20.	SO+1y	nil	DE
PIB	**-07**	**Unsolicited offers of service - not considered** (covers résumés) NOTE: This secondary covers unsolicited résumés and similar personal offers of service that were not considered. Applications and résumés of applicants under consideration are classified under secondary -20.	SO	nil	DE
	-20	**Staffing competition files** (arrange by competition) (covers correspondence, applications, résumés, job descriptions, posting request forms, job postings, eligibility lists, and tests) SO: upon the date the successful applicant is placed into new position (i.e., the effective date of the appointment), and if an eligibility list or inventory has been established, when the list has been exhausted or the term of the list has expired, whichever is earlier 2y: The retention period satisfies reference requirements and ensures that personal information used to make a decision that directly affects an individual is retained for at least one year. NOTE: These files include candidates' qualifications, scores, and test results, competition assessment tools including criteria and rating methodology, copies of approvals or waivers for special considerations or restrictions, reference check procedures and ranking guides, decisions, copies of offer letters, and letters of regret and feedback to unsuccessful candidates. NOTE: Original applications and résumés of successful candidates are filed on the relevant employee personnel files (see 7385-20). Copies are retained on the competition files.	SO+2y	nil	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7730 TRAINING AND DEVELOPMENT

Records relating to the development and delivery of agency training sessions, workshops, courses, professional development and information sessions.

Record types include correspondence, reports, instructor's notes, presentation slides, handouts, course workbook and manuals, class lists, and evaluation forms.

For training budget, see *ARCS* primary 1000.
For human resources topical files, see secondary 7300-06.

The OPR is ( ) unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-00	**Policy and procedures**	SO	5y	FR
-01	**General**	CY+1y	nil	DE
-02	**Career development paths**	SO	nil	DE
-03	**Educational leave criteria**	SO	nil	DE
-04	**Employee orientation information**	SO	nil	DE
-05	**Training and skills needs analysis**	SO	nil	DE
-06	**Training evaluations**	SO	nil	DE
-07	**Training packages** NOTE: This secondary covers the final version of instructor's/facilitator's notes, presentation slides, handouts, and participant workbooks and manuals. The development of this material is covered by secondary -20.	SO	2y	DE
-20	**Training development files** (arrange by course name)	SO	2y	DE
-25	**Training implementation history files** (arrange by course name) NOTE: This secondary covers course requests and information relating to the implementation history of particular courses, including facilities, aids and resources used.	SO	2y	DE

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

7730 TRAINING AND DEVELOPMENT

			A	SA	FD
	-30	**Training session attendance files** (arrange by course, then by delivery date)	SO	nil	DE

END OF PRIMARY

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

SUBJECT HEADINGS PRIMARY NUMBERS

HUMAN RESOURCES ARCS SUPPLEMENT (HRAS)

INDEX

This index is an alphabetical guide to *ORCS* subject headings and relevant primary number(s).

Use this index in the following ways:
- to locate the correct primary number to classify documents;
- to retrieve, by subject, documents which have been classified and filed; and
- to access the contents of your *ORCS*.

This index contains an alphabetical listing of:
- all keywords from secondary titles;
- keywords from primary scope notes;
- common synonyms for indexed keywords; and
- common abbreviations.

Cross-references:

"See" references indicate that the subject heading sought is indexed under an alternate entry (a more appropriate keyword, a full or official name, etc.).

"See also" references are used when additional information can be found in another entry.

Key to *ARCS/ORCS* Codes and Acronyms

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

SUBJECT HEADINGS	PRIMARY NUMBERS
- A -	
ACCOUNTING	
- payroll	7550
AGREEMENTS	
- collective	7480
APPEALS	
- awards	7310
- disputes/complaints	7480
- job classification	7360
ASBESTOS	
- exposure	7560
AWARDS	
- applicant/recipient files	7310
- program information files	7310
- B -	
BALANCING	
- payroll	7550
BARGAINING	
- collective	7480
BENCHMARKS	
- job	7360
BENEFITS	
- administration	7315
- disability	7315
- employee counseling services	7315
- employment insurance	7315
- family counseling services	7315
- health	7315
- life insurance	7315
- plan information	7315
- retirement and pension	7315
- salary and retirement savings plans	7315
- workers' compensation	7315
BIOLOGICAL	
- hazard exposure files	7560
BONUS PROGRAM	
- calculations	7360
- C -	

Key to *ARCS/ORCS* Codes and Acronyms

SUBJECT HEADINGS	PRIMARY NUMBERS
CAMPAIGNS	
- planning	7320
- Provincial Employee Community Services	7320
CANADA REVENUE AGENCY	
- account reconciliation	7550
CARRIERS	
- benefit	7315
CHARITABLE DONATIONS	
- campaign planning	7320
- disbursement records	7320
- donor reconciliation records	7320
CLASSIFICATION OF POSITIONS	
- appeals	7360
- benchmarks	7360
- job evaluation plans	7360
COLLECTIVE	
- agreements	7480
- bargaining	7480
COMMUNITY	
- services fund	7320
COMPENSATION	
- bonus program	7360
- incentive pay program	7360
- job evaluation	7360
- perquisite allowances	7360
- salary schedules	7360
COMPETENCY	
- job profiles	7360
COMPETITIONS	
- case files	7665
- criminal record check consent forms	7665
- model interview questions	7665
- selection standards	7665
- student recruitment	7665
- unsolicited offers of service	7665
COMPLAINTS	
- resolution	7480
COURSES	7730
CRA (See CANADA REVENUE AGENCY)	

Key to *ARCS/ORCS* Codes and Acronyms

SUBJECT HEADINGS	PRIMARY NUMBERS
CRIMINAL RECORD CHECK	
- consent forms (hired)	7385
- consent forms (not hired)	7665
- D -	
DISABILITY	
- benefits	7315
- case management	7315
DISBURSEMENTS	
- charitable donation	7320
DISCRIMINATION	
- complaints	7480
DISPUTE RESOLUTION	
- dispute/complaint resolution files	7480
DONATIONS	
- charitable	7320
- E -	
EMPLOYEE	
- awards	7310
- benefits	7315
- charitable donations	7320
- complaints	7480
- counseling services	7315
- disability	7315
- dispute/resolution files	7480
- engagement	7480
- grievances	7480
- learning	7730
- pay files	7550
- performance evaluations	7385
- personnel files	7385
- recognition	7310
- recruitment	7665
- training and development	7730
- work history	7385
EMPLOYER-EMPLOYEE RELATIONS	
- collective agreement	7480
- collective bargaining negotiations	7480
- disputes/complaints	7480
- employee engagement	7480
- essential services planning	7480
- labour relations	7480
- strike planning	7480

Key to *ARCS/ORCS* Codes and Acronyms

SUBJECT HEADINGS	PRIMARY NUMBERS
EMPLOYMENT	
- employment equity topical files	7300
- insurance	7315
ENGAGEMENT	
- employee	7480
ERGONOMIC ASSESSMENTS	7560
ESSENTIAL SERVICE	
- planning	7480
EXCLUDED EMPLOYEES	
- dispute resolution	7480
- negotiations	7480
EXIT PROGRAMS	7580
EXPOSURE FILES	
- biological hazard	7560
- F -	
FAMILY	
- counseling services	7315
FIRST AID	
- logs	7560
- needs assessments	7560
- treatment books	7560
- G -	
GENERIC	
- job files	7360
GRIEVANCE(S)	7480
- H -	
HARASSMENT	
- complaints	7480
HEALTH	
- benefits	7315
- employee case files	7560
HEPATITIS B	
- vaccinations	7560
HIRING	7665

Key to *ARCS/ORCS* Codes and Acronyms

SUBJECT HEADINGS	PRIMARY NUMBERS
HUMAN RESOURCES	
- employee files	7385
- policy development files	7300
HUMAN RIGHTS	
- topical files	7300
- I -	
INSURANCE	
- employment	7315
- life	7315
INTERPRETATIONS	
- collective agreement	7480
- J -	
JOB DESCRIPTION	
- appeals	7360
- benchmarks	7360
- classification review	7360
- evaluation plans	7360
- position history	7360
- salary schedules	7360
- topical files	7360
JOB ENHANCEMENT	
- topical files	7300
- K -	
- L -	
LABOUR RELATIONS	
- bargaining	7480
- complaints	7480
- disputes	7480
LATENT	
- biological hazard files	7560
LEARNING	
- development files	7730
- employee orientation	7730
- implementation files	7730
- session attendance files	7730
LONG TERM DISABILITY	
- disability	7315
LTD (See LONG TERM DISABILITY)	

Key to *ARCS/ORCS* Codes and Acronyms

SUBJECT HEADINGS — PRIMARY NUMBERS

- M -

- N -

NEEDS ASSESSMENT
- first aid 7560
- learning 7730

- O -

OCCUPATIONAL SAFETY AND HEALTH
- employee health files 7560
- first aid needs assessments 7560
- first aid treatment books and logs 7560
- hazardous material information 7560
- latent biological hazard exposure 7560
- OSH inspection files 7560
- OSH program information 7560
- personal protective equipment 7560
- refusal to work because of unsafe conditions 7560
- work-related incidents 7560

- P -

PACKAGES
- training 7330

PAYROLL
- accounting reports 7550
- balancing reports 7550
- batch control 7550
- Canada Savings Bond 7550
- CRA account reconciliation 7550
- employee pay files 7550
- pay files 7550
- pay run batch control 7550
- reports 7550

PERSONNEL (see HUMAN RESOURCES)

POLICY
- development 7300

PLANNING
- charitable donation campaigns 7320
- essential service 7480
- staffing requirements 7580

POSITION
- classification 7360
- history files 7360

SUBJECT HEADINGS	PRIMARY NUMBERS
POSTINGS	
- job	7665
PROGRAM MANAGEMENT	
- awards	7310
- bonus pay	7360
- employee recognition	7310
- health	7560
- occupational safety	7560
PROVINCIAL	
- Employee Community Services Fund	7320
- Q -	
- R -	
RECOGNITION	
- applicant/recipient files	7310
- program information files	7310
RECONCILIATION	
- charitable donation	7320
RECORD CHECKS	
- criminal	7385,7665
RECRUITMENT	
- model interview questions	7665
- selection standards	7665
- student	7665
- unsolicited offers of service	7665
- competitions	7665
REPORTS	
- employee recognition	7310
- payroll	7550
- staff projection	7580
- work related incident	7560
- S -	
SAFETY	
- occupational	7560
SALARY	
- bonus pay program	7360
- incentive pay program	7360
- perquisite allowance	7360
- schedule	7360

Key to *ARCS/ORCS* Codes and Acronyms

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

SUBJECT HEADINGS	PRIMARY NUMBERS
SEXUAL HARASSMENT	
- complaints	7480
SHORT TERM ILLNESS AND INJURY PLAN	
- disability	7315
STAFFING	
- competitions	7665
- criminal record check	7665
- model interview questions	7665
- planning	7580
- projections	7580
- requirements	7580
- selection standards	7665
- seniority	7580
- student recruitment	7665
- unsolicited offers of service	7665
- vacancy lists	7580
STIIP (see SHORT TERM ILLNESS AND INJURY PLAN)	
STRIKE	
- planning	7480
STUDENT	
- recruitment	7665
SUCCESSION PLANNING	
- staffing requirements	7580
- T -	
TRAINING	
- career development paths	7730
- development files	7730
- educational leave	7730
- employee orientation	7730
- evaluations	7730
- packages	7730
- skills needs analysis	7730
- U -	
- V -	
- W -	
WCB (see WORKERS' COMPENSATION)	
WOMEN'S ISSUES	
- topical files	7300

Key to *ARCS/ORCS* Codes and Acronyms

This records schedule is approved in accordance with the *Document Disposal Act* (RSBC 1996, c. 99) and constitutes authority for retention and disposition of the records it covers. Consult your Records Officer.

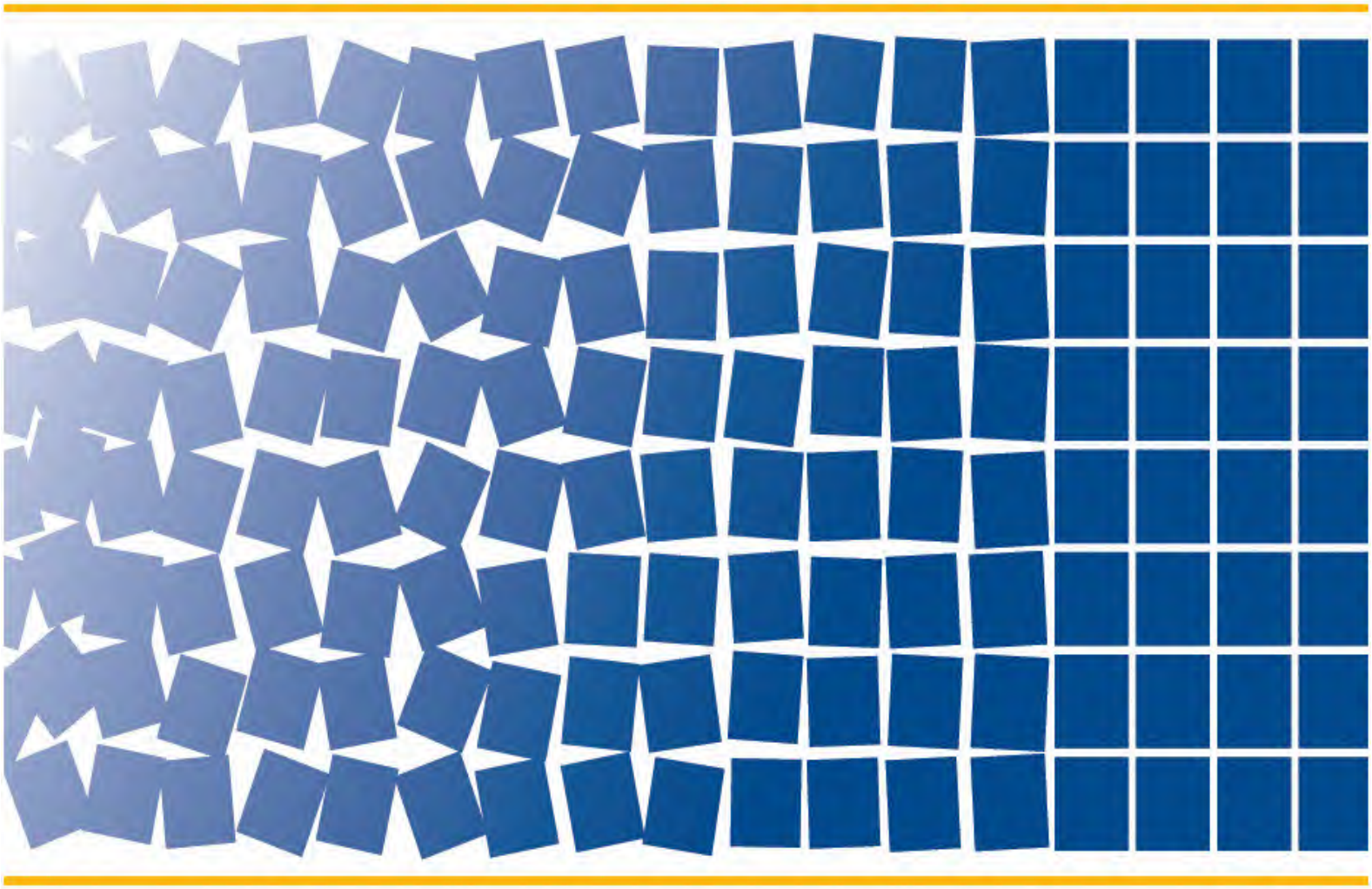
SUBJECT HEADINGS	PRIMARY NUMBERS
WORK HISTORY	
- employee	7385
WORKERS' COMPENSATION	7315
WORKFORCE	
- planning	7580

- X -

- Y -

- Z -

OIL AND GAS REGULATION OPERATIONAL RECORDS CLASSIFICATION SYSTEM



BRITISH COLUMBIA

OIL AND GAS COMMISSION

OIL AND GAS REGULATION

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

TABLE OF CONTENTS

USEFUL INFORMATION

EXECUTIVE SUMMARY

SECTION 1 20000 – 21900 OIL AND GAS REGULATION

SYSTEMS SECTION

APPENDIX A SUMMARY OF AMENDMENTS

APPENDIX B SUMMARY OF RETENTIONS

USEFUL INFORMATION

Key to Information Schedule Codes and Acronyms:

Information Schedule titles:	***ARCS*** = *Administrative Records Classification System* ***ORCS*** = *Operational Records Classification System*
Office information:	**OPR** = Office of Primary Responsibility
Records life cycle:	**A** = Active **SA** = Semi-active **FD** = Final Disposition
Active and semi-active period codes:	**CY** = Calendar Year **FY** = Fiscal Year **NA** = Not Applicable **SO** = Superseded or Obsolete **w** = week **m** = month **y** = year
Final disposition categories:	**DE** = Destruction **FR** = Full Retention **SR** = Selective Retention **OD** = Other Disposition **NA** = Not Applicable
Special flags:	**FOI** = Freedom of Information/Protection of Privacy **PIB** = Personal Information Bank **VR** = Vital Records

The following links provide additional resources for managing your information:

- *ARCS and ORCS User Guide*.
- Special schedules for records that are not covered by *ARCS* and *ORCS*.
- Legislation, policies, and standards for managing records in the BC Government.
- Tips, guides, and FAQs on related topics.
- Records Officer contact information.

BRITISH COLUMBIA Ministry of Citizens' Services

Schedule No: 163507
Amendment No: 144019

INFORMATION SCHEDULE APPROVAL

Title: *Oil and Gas Regulation Operational Records Classification System (ORCS)*

Oil and Gas Commission

Scope of Schedule:

This *ORCS* amendment updates the classification system and retention and disposition schedule for the operational records of the Oil and Gas Commission under the *Oil and Gas Activities Act* (SBC 2008, c. 36) and associated regulations, the *Environmental Management Act* (SBC 2003, c. 53), the *Forest Act* (RSBC 1996, c. 157), the *Heritage Conservation Act* (RSBC 1996, c. 187), the *Land Act* (RSBC 1996, c. 245), and the *Water Sustainability Act* (SBC 2014, c. 15).

The *ORCS* classifications and retentions apply to all relevant digital and physical operational records, both in the office and in storage. Records under a closed secondary may finish their lifecycle with the original retention.

The retention periods specified in this schedule meet all operational, fiscal, legal, and audit requirements.

For more information, see the attached schedule.

Earliest date of records covered by this schedule: 1945

The government body endorses this schedule and its implementation.

Government body endorsement — Date: 01/03/2019
Name: LEN DAWES

The Information Management Advisory Committee recommends this schedule for approval.

Susan Laidlaw, Chair — Date: 20 Mar 2019

APPROVED BY THE CHIEF RECORDS OFFICER:

Joel Fairbairn — Date: 21 Mar 2019

The attached schedule was developed in consultation with staff and managers who conduct the operational functions in the creating agency. It has also been reviewed by appropriate Government Records Service staff to ensure it meets scheduling and appraisal standards, and reflects sound recordkeeping practices.

Schedule Developer: Mahia Frost
Archivist: Joni Mitchell

Endorsed by Government Records Service.

Alexander Wright, Chief Archivist
Date Dec. 17, 2018

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

A SA FD

OIL AND GAS REGULATION

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

EXECUTIVE SUMMARY FOR AMENDMENT 1

This *ORCS* amendment updates the classification system and retention and disposition schedule for the operational records of the Oil and Gas Commission under the *Oil and Gas Activities Act* (SBC 2008, c. 36) and associated regulations, the *Environmental Management Act* (SBC 2003, c. 53), the *Forest Act* (RSBC 1996, c. 157), the *Heritage Conservation Act* (RSBC 1996, c. 187), the *Land Act* (RSBC 1996, c. 245), and the *Water Sustainability Act* (SBC 2014, c. 15).

This amendment reflects current Commission business practices and requirements, embodies modern ORCS standards, and aligns with legislative changes made since the original ORCS was approved in 2005.

It is the first phase in a two-part ORCS modernization project. Amendment 1 readies the Commission for its goal of using an Electronic Document Records Management System (EDRMS), and managing its digital records, while still taking care of the physical records that remain in Commission custody. The second phase will address the Commission's complex system environment and create comprehensive system data management plans.

The ORCS classifications and retentions apply to all relevant digital and physical operational records, both in the office and in storage. Records under a closed secondary may finish their lifecycle with the original retention (see Appendix A for details regarding closed secondaries). Active and semi-active retention periods meet operational, administrative, legal, fiscal, and audit requirements, and the final dispositions ensure that records with enduring evidential and historical values are preserved.

This executive summary highlights records held longer than seven years in the Commissions' custody, and those to be retained by the government archives. The information is grouped in categories to aid in understanding significant aspects of the schedule. Primary and secondary numbers link record categories to the ORCS; please consult relevant primaries for further information.

Executive summary categories:

New classifications with long-term retentions	page 2
New classification for records transferring out of government custody	page 3
Original classifications with changed final disposition	page 4
Original classifications where retention has increased	page 4
Classifications with inter-dependent retentions	page 4

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

	A	SA	FD

NEW CLASSIFICATIONS WITH LONG-TERM RETENTIONS:

1) Reservoir analysis and management (21400-35) — SO nil FR

Commonly called the “field and pool files”, this secondary covers records relating to the approval and monitoring of projects related to managing and analysing reservoir contents. It also covers records that document the reservoir properties, characteristics and boundaries.

The files are closed according to the following criteria, after which they will be transferred to the government archives:

- for records relating to production management, such as Good Engineering Practices (GEPs), 20 years after pool abandonment;
- for records relating to projects that resulted in a changed subsurface environment or have potential safety considerations in future activities, such as disposals and waterflood projects, when no longer required in the Commission’s custody to provide evidence of the activities;
- for records which document the composition and structure of the field or pools, when that information is no longer required.

2) Major incident and emergency response files (20750-50) — SO nil FR

These incidents may potentially affect life and safety, warrant full investigation, or are managed through the Emergency Operations Centre (EOC).

The files are kept until the incident and response is complete, the information is no longer relevant for site reclamation, and are then transferred to the government archives.

3) Contravention decisions and orders (20300-60 and 65) — SO+10y nil FR

These are the decision files for administrative findings of contravention, per the *Administrative Penalties Regulation* (B.C. Reg. 35/2011), and the issuance of orders to enforce a company’s compliance with legislation and regulation, to mitigate risk to public safety, to protect the environment, or to promote the conservation of petroleum and natural gas resources.

The files are kept for 10 years after administrative penalties have been paid, or the conditions of the order have been satisfied, and the review and appeal periods have expired. Then they are transferred to the government archives.

4) External audit and compliance assessment records

20550-10 — CY+10y nil DE

20550-20 — SO nil DE

These are records of the Commission’s audit programs, which evaluate a permit holder’s activities, programs, and/or management systems against established criteria.

	A	SA	FD

The audit working files are kept for 10 years to provide reference in subsequent audits, and the final reports are kept until they are no longer required for tracking a company's history of compliance with their regulatory requirements.

5) Emergency management company correspondence (20750-05) CY+9y nil DE

This correspondence covers approvals/amendments for emergency response plans, timelines for emergency response exercises, and variances for regulatory requirements.

The files are kept for 10 years to ensure that the correspondence is retained for a similar period as the associated exercises and emergency response plans, and that the company's compliance/activity information is available in support of determining administrative penalties.

NEW CLASSIFICATION FOR RECORDS TRANSFERRING OUT OF GOVERNMENT CUSTODY

1) Corporate asset files for transferred assets (20850-21) SO nil OD

These corporate asset files are received from insolvent or at risk companies whose assets may potentially be orphaned, to support the future transfer of the asset to a responsible party and prevent the site from being orphaned. Many parts of the corporate file duplicate the Commission's files, and hold no value to the Commission, yet have great value to the receiving company so they may understand the operations and details of the assets they are acquiring.

The file will be transferred to the responsible party / new permit holder when the ownership of the asset has been transferred, to assist in the ongoing management and eventual reclamation of the site.

ORIGINAL CLASSIFICATIONS WITH CHANGED FINAL DISPOSITION

1) Indigenous relations (20100-20) SO nil FR

The final disposition for this category changed from selective retention (SR) by the government archives to full retention (FR). The original classification included permit-specific indigenous consultation working files, but defined them as eligible for destruction because the record of consultation is preserved on the permit application file. Those permit-specific working files are now classified under a different secondary, and the original records selected for full retention are the only records being covered here.

2) External communication products (21600-06) CY+3y 6y FR

The final disposition for this category changed from destruction to full retention by the government archives. This is consistent with the full retention of communication projects in the *Government Communication ORCS*. It also reflects the fact that the records provide evidence of the information conveyed by the Commission to clients, Indigenous peoples, communities and multiple levels of government about oil and gas operations and activities in British Columbia, and the methods and tools used to communicate that information.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

	A	SA	FD

ORIGINAL CLASSIFICATIONS WHERE RETENTION HAS BEEN INCREASED

1) Enforcement case files (20300-40) — CY+14y nil DE

The retention for these files has lengthened to 15 years to ensure that the case file is available when establishing administrative penalties, and that it remains available while associated contravention decisions and orders are open.

2) Corporate Registry (20000-20) — SO nil DE

The original classification for these “company files” did not have a defined closing trigger. This has been updated to keep the records until five years after the company is no longer active in the province, or for longstanding companies, when 12 calendar years has elapsed from the receipt of the information. This ensures the information is available if a company restarts activities, and retaining 12 years of longstanding company information is consistent with the name change and amalgamation records classified under 20200-18.

CLASSIFICATIONS WITH CONNECTED RETENTIONS

The classifications in this category were in the original *ORCS*, and document core Commission functions. The retentions have changed, and closing triggers clarified, but they are grouped together in this summary to highlight that their retentions are linked to each other.

To begin, a primary function of the Commission is to process applications for oil and gas and related activities:

Application Files (20200-20) — SO nil SR

Covers all permit and license applications received and approved by the Commission. These records are kept until all permits and licences have expired, conditions have been met, and, where relevant, the retentions in the associated activity files have expired.
The exceptions to this are archaeological permits, which are kept until no longer required to provide evidence of permitted archaeological activities.
Most application files will be transferred to the government archives.

For most of the applications in the Commission, once an application is approved there is an associated “activity” file, which holds the ongoing monitoring and technical material related to the activity. The application file is held for the duration of the activity file. These are the activity file retention plans:

Facility files (20300-30): kept until the facility has been removed, the site has been restored, and the file is no longer required to document activities conducted on the site. Then they are transferred to the government archives.

Road files (20900-20): kept for 5 years after the road has been cancelled or deactivated, and restoration is complete. Then they are transferred to the government archives.

A SA FD

Pipeline projects (21000-35): kept until the pipeline has been removed, or no longer exists. Then they are transferred to the government archives.

Well files (21900-30): kept until a certificate of restoration is issued, and the well information is no longer needed for environmental and safety management. Then they are transferred to the government archives.

These categories of records also connect to the activity files:

1) Inspection records (20300-30) SO nil DE

Covers site inspections performed on activities such as wells, pipelines, facilities, roads, bridges, dams, crossings, rigs and more; some of which are tied to an activity file, and some more "general" and associated to a company. Inspections associated with a permitted activity are kept as long as the associated activity file (e.g., well file) is kept; more general inspections that are not connected to a permitted activity are kept for 10 years after remediation actions are completed.

2) Incident files (20750-45) SO nil DE

Covers minor incidents and lower level emergencies that are the result of an oil and gas activity; these may be spills, equipment failures or small fires. Incident records are kept until the incident and follow up activities are complete, and the information is no longer relevant for site reclamation. Major incidents (page 2) are also kept until the information is no longer relevant for site reclamation.

ALL OTHER ORCS CLASSIFICATIONS DE

All other records are destroyed at the end of their semi-active retention periods. The retention of these records varies depending on the nature of the records and the function performed, but does not exceed seven years. Any information from these records that has ongoing value is adequately documented under secondaries with longer retentions and/or full or selective retention appraisals within the ORCS or in ARCS, such as summary reports, policy records, executive briefing notes (*ARCS* secondary 280-20), and annual service plan reports (*ORCS* secondary 21600-20). These records have no enduring value to government at the end of their scheduled retention periods.

END OF EXECUTIVE SUMMARY

SECTION 1

OIL AND GAS REGULATION

PRIMARY NUMBERS

20000 – 21900

Section 1 covers records relating to the regulation of oil and gas activities, related activities and certain approvals relating to NEB pipelines in British Columbia by the Oil and Gas Commission. This includes: the review of permit applications to ensure that approved applications are in the public interest and have regard to environmental, economic and social effects; encouraging the participation of communities, landowners and Indigenous peoples in processes affecting them; compliance and enforcement activities to ensure safe and efficient practices; participating in planning processes; and delivering programs of education and communication for stakeholders.

The Commission is a crown corporation that exercises authorities pursuant to a number of enactments, including:

- The *Oil and Gas Activities Act* (SBC 2008, c. 36) and its associated regulations, to regulate through permits, authorizations, orders and regulations, oil and gas and related activities in B.C., including wells, facilities, oil refineries, natural gas processing plants, pipelines and oil and gas roads.
- The *Environmental Management Act* (SBC 2003, c. 53), and the *Oil and Gas Waste Regulation* (B.C. Reg. 254/2005), to regulate oil and gas waste permits, such as air emissions. The *Environmental Management Act* also delegates authority to act as Special Conservation Officers to regulate environmental protections.
- The *Petroleum and Natural Gas Act* (RSBC 1996, c. 361) and associated regulations which, for example, regulate subsurface tenures and royalties for oil and gas, or terms and conditions of surface leases.
- The *Forest Act* (RSBC 1996, c. 157), to regulate oil and gas Master Licences to Cut, cutting permits and use of forestry roads.
- The *Heritage Conservation Act* (RSBC 1996, c. 187), to regulate cultural and heritage (archaeology) sites in the province.
- The *Geothermal Resources Act* (RSBC 1996, c. 171), and associated regulations, to regulate development and use of geothermal resources
- The *Land Act* (RSBC 1996, c. 245), to regulate Crown land licences of occupation, statutory right of ways and rents.
- The *Water Sustainability Act* (SBC 2014, c. 15), to regulate water diversion, storage and use of water through issuance of water licences and regulation of any associated dams.

- The *Agricultural Land Commission Act* (SBC 2002, c. 36), to regulate the non-farm use of land in the Agricultural Land Reserve for oil and gas purposes.
- The *Mines Act* (RSBC 1996, c. 293) to regulate extraction of aggregates.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

SECTION 1 TABLE OF CONTENTS

OIL AND GAS REGULATION

20000 - 21900

20000 OIL AND GAS REGULATION – GENERAL

20100 INDIGENOUS RELATIONS

20200 APPLICATION REVIEW

20250 ARCHAEOLOGICAL ACTIVITY MONITORING (NEW)

20300 COMPLIANCE AND ENFORCEMENT

20550 EXTERNAL AUDIT AND ASSESSMENT (NEW)

20600 FACILITIES REGULATION AND MONITORING

20750 INCIDENT AND EMERGENCY RESPONSE (NEW)

20850 LIABILITY MANAGEMENT (NEW)

20900 ROAD REGULATION AND MONITORING

21000 PIPELINE REGULATION AND MONITORING

21100 POLICY AND PROCEDURES DEVELOPMENT

21400 RESERVOIR REGULATION AND MONITORING

21600 STAKEHOLDER RELATIONS

21700 TIMBER CUTTING LICENSING

21900 WELL REGULATION AND MONITORING

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20000 OIL AND GAS REGULATION – GENERAL

Records not shown elsewhere in this *ORCS* that relate generally to regulation of the oil and gas industry and the activities of the Commission. Covered in this primary are general records categories that apply to all staff in the Commission, such as notebooks, ad hoc advisory material, and the Commissions' website. The corporate registry tracks information regarding companies with assets in British Columbia.

This primary also covers the board of directors' records. The board of directors manage the affairs of the Commission, provide guidance, approves budgets, service plans and regulatory initiatives, pass regulations per the *Oil and Gas Activities Act* (SBC 2008, c. 36, s.106-109) , and establish the Commission's organizational structure.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS*.
For convenience copies, and routine reports of temporary usefulness, see special schedule 102901 (Transitory Records).
For legal opinions, see *ARCS* primary 350.
For legislation and regulations, see *ARCS* primaries 125-140.
For policies, procedures, standards, and guidelines, see secondary 21100-00.
For program planning, see *ARCS* secondary 400-20.
For publications such as *The Pipeline*, see *ARCS* primary 312.
For reference material/topical files, see *ARCS* secondary 358-20.
For tracking lists, spreadsheets and registers, see *ARCS* secondary 100-05.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE

NOTE: Throughout this section, this secondary covers miscellaneous records that relate to the primary but do not document decisions and actions, and do not relate to topics that warrant specific classifications.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20000 OIL AND GAS REGULATION – GENERAL

		A	SA	FD
-02	**Ad hoc analysis projects** (covers ad hoc, issue driven projects, which may include technical analysis, advisory services, or assessing potential impacts of change in policy, regulation, industry, etc.) SO: if related to a plan or policy, when it has been abandoned or approved and there is no need to reference the records; for all other ad hoc analysis projects, when it no longer has reference value NOTE: This secondary applies to records of advisory and analysis work done throughout the Commission, sometimes with the sector, municipalities, or ministries. Examples of these projects would be: compliance and enforcement's equipment inventory; evaluating the status of dams when legislation changed; resource assessments; or assessing the potential impact government's policies and plans, such as land use planning, would have on Commission processes. This secondary does not apply to studies, major projects, permit-specific work, or field and pool technical analysis. NOTE: Classify project records relating to business or program planning under *ARCS* 400, and strategic engagement projects under secondary 21600-35.	SO	nil	DE
-06	**Notebooks** (covers staff notebooks containing day to day planning, meeting notes, assignments, and field notes; these are used to support compliance, investigations or to provide background information in subsequent situations) SO: when no longer necessary for reference purposes NOTE: Where there is a consistent practice of transcribing notes of inspections, investigations, or stakeholder conversations into the official file (usually in a system such as KERMIT) the original notebook/notes can be considered transitory. For notebooks that are not transcribed, and document conversations with First Nations, community, industry, or investigations, notebooks must be kept as long as necessary for providing continuity in relationship, documentation of conversation, and reference.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20000 OIL AND GAS REGULATION – GENERAL

		A	SA	FD
-07	**Oil and Gas Commission website** (http://www.ogc.gov.bc.ca/) SO: when the website is altered, updated, redesigned, or closed DE: As the website is updated, superseded/obsolete versions of documents on it may be destroyed in accordance with approved retention schedules. When the website is closed, it can be destroyed after relevant schedules have elapsed and/or the documents have been classified elsewhere. NOTE: All documents presented on this website are classified under appropriate secondaries within this *ORCS* or in *ARCS*.	SO	nil	DE
-10	**Statistical and activity reports** (covers ad hoc, statistical and routine reports that are not part of an operational file, such as a compliance file or well file) SO: when information is no longer required for statistical, reporting, or analysis purposes NOTE: This secondary covers the various reports produced by the Commission, such as weekly/monthly/quarterly reports, which are not classified elsewhere in this *ORCS*. It does not cover, for example, annual reports, service plans and annual activity reports, which are classified under secondary 21600-20, or technical/data reports for operational activities such as wells or pipelines, which belong on the individual activity file.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20000 OIL AND GAS REGULATION – GENERAL

			A	SA	FD
	-20	**Corporate registry** (formerly called “company files”, this secondary covers information about specific companies such as address changes, company approvals, copies of insurance, and other company information) (arrange by company name) SO: when it has been five years since the company ceased operation in the province, or for longstanding companies, when 12 calendar years have elapsed from the receipt of the information NOTE: The retention ensures the information is available if a company restarts activities; in this event, the company is reinstated and the file reactivated. Retaining 12 years of longstanding company information is consistent with the name change and amalgamation file under 20200-18. DE: Information about companies will be destroyed because it is also in the application (20200-20) and related activity files.	SO	nil	DE
	-35	**OGC Board of Directors files** (includes board briefing material, such as agendas, minutes, presentations, and reports) 10y: The combined active and semi-active retention period of ten years is in keeping with special schedule 102906 (Executive records). FR: The government archives will fully retain OGC Board of Directors case files because they provide evidence of how the Board guides the affairs of the Commission and approves the Commission’s budget, service plans, and regulatory initiatives.	FY+1y	8y	FR

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20000 OIL AND GAS REGULATION – GENERAL

		A	SA	FD
-40	**Compliance evaluation files** (covers the assessment and evaluation of a company's compliance with regulatory requirements; this is sometimes done in conjunction with the Compliance and Enforcement team and is more of a "compliance support" working file, and other times the compliance evaluation is performed independently, such as archaeology's non-compliance files) (arrange by company, then by year) SO: when outstanding issues have been resolved, and when no longer useful for researching a company's compliance history NOTE: This secondary does not cover compliance and enforcement investigations and inspections, which are are classified under primary 20300, or audits, which are classified under primary 20550. DE: Compliance evaluation records will be destroyed because they serve as working files done in conjunction with the Compliance and Enforcement Branch (20300). Archaeology compliance evaluations will be destroyed because the functions and activities are sufficiently documented in the applications (20200-20) and enforcement actions related to non-compliance are fully retained under contravention decisions and orders (20300-60 and -65).	SO	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20100 INDIGENOUS RELATIONS

Records relating to communication and engagement with Indigenous communities to identify the impact of oil and gas development activities on those communities, and to promote a resolution of those impacts. The Commission works with communities to: assist with their understanding and involvement in decisions which may affect their interests; develop the capacity to participate in the review and approval of oil and gas projects; act as a facilitator between industry and Indigenous peoples, and enter agreements with Indigenous communities.

To support Indigenous peoples' participation in processes affecting them and to build relationships, Commission staff facilitate meetings with senior leadership and statutory decision makers, take part in community visits and participate in community events, and identify two-way training and information sharing opportunities to enhance relationship building and mutual understanding of interests. Commission staff also consult with Indigenous communities on proposed oil and gas activities for which the Commission has received an application. Multiple groups may be consulted in relation to an individual application.

For capacity funding agreement negotiation and management, see *ARCS* primary 146.
For engagement surveys, see *ARCS* 338.
For memoranda of understanding and agreement development and negotiation, see *ARCS* primary 146.
For operational policy, procedures, and protocol, including the *Compendium*, see secondary 21100-00.
For permit-specific application review working files, see 20200-40.
For reference material/topical files, see *ARCS* secondary 358-20.
For regulatory development see *ARCS* primary 140.
For strategic projects, see secondary 21600-35.
For tracking sheets and lists, such as the election schedule or First Nation consultation spreadsheet, see *ARCS* secondary 100-05.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20100 INDIGENOUS RELATIONS

		A	SA	FD
-20	**Indigenous relations** (includes reports, copies of agreements, compliance and enforcement complaints, correspondence, issue resolution, meeting notes, maps, photos, and guidance documents) (arrange by band, consultancy, community, or tribal council) SO: when no longer required to support the Commissions relationship and provide immediate access to its history with Indigenous communities FR: The government archives will fully retain Indigenous relations records because they provide evidence of the Oil and Gas Commission's consultation and liaison with Indigenous groups that are or may be affected by natural resource sector activities. Indigenous relations records specific to a particular application are documented on the relevant application file, which is fully retained under secondary 20200-20. NOTE: Permit-specific Indigenous consultation records are classified and managed accordingly: consultation working files, kept for reference, are classified under 20200-40, and the record of consultation is fully retained in the application file under 20200-20.	SO	nil	FR
-40	**Cultural awareness and training** (covers cultural and relationship building events and training, both internal and external; this includes cultural awareness workshops such as community events, culture camp, OGC 101, as well as multi-agency and internal cross-cultural initiatives and training opportunities) (arrange by event, workshop or initiative name, and then year) SO: when no longer used or referenced	SO	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20200 APPLICATION REVIEW

Records relating to the review of all industry applications and proposals seeking issuance of permits, licenses and approvals as they pertain to oil and gas activities. The Commission is responsible for ensuring that approved applications are in the public interest with regard to environmental, economic and social impacts. Application files are historically known as “OGC” files.

The Commission’s specific permitting authority is defined in the *Oil and Gas Activities Act* (SBC 2008, c. 36) (*OGAA*). In order to function as a single-window regulator for oil and gas activities in British Columbia, delegation agreements are in place to allow the Commission to make decisions on certain oil and gas uses. In addition, authorizations granted through specific acts provide the Commission permitting powers under specified enactments.

Permits and authorizations granted by the Commission include:

- Oil and gas activity permits under *OGAA*, including well, pipeline, facilities, road and geophysical permits.
- Associated oil and gas activity authorizations under the *Petroleum and Natural Gas Act* (RSBC 1996, c. 361) or *Land Act* (RSBC 1996, c. 245), as applicable, including activities such as investigative use, aggregate operations, work spaces and camp sites.
- Authorizations and approvals under the *Water Sustainability Act* (SBC 2014, c. 15), including authorizations and approvals for changes in and about a stream, short-term water use and water licences.
- Non-farm use of lands included in the Agriculture Land Reserve (ALR), under delegated authority under the *Agriculture Land Commission Act* (SBC 2002, c. 36).
- Master licences to cut, cutting permits, and road use permits under the *Forest Act* (RSBC 1996, c. 157).
- Archaeology-related permissions under the *Heritage Conservation Act* (RSBC 1996, c. 187).
- Specific provincial authorizations related to pipelines subject to the *National Energy Board Act* (R.S.C., 1985, c. N-7).
- Approvals and permits for waste treatment and disposal by the oil and gas industry per the *Environmental Management Act*, (SBC 2003, c. 53).

The application review process of these permits and authorizations consists of a sequence of steps. A company submits an application, which includes consultation and technical information. The application is reviewed for impacts affecting stakeholders, Indigenous communities, environmental issues and archaeological interests. Enhanced consultation may be required, including: public safety and emergency response planning; records of community input; assessing commitments by applicant; and comments provided by the application review team. The majority of applications are processed through the Application Management System (AMS); see the Systems Section for an overview of how the system manages application processing.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20200 APPLICATION REVIEW

	A	SA	FD

Approved oil and gas applications give permission to the company to carry out construction and operations pertinent to the activity. The permit expires where construction activities have not started within two (2) years of permit issuance. Unless expired, the permit remains active until cancelled, suspended or declared spent.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a description of the Application Management System (AMS), Integrated Resource Information System (IRIS), and KERMIT, see the Systems Section.
For declined, cancelled or withdrawn archaeological permits, see secondary 20250-20.
For General development permits, see *Appendix A: Summary of amendments*.
For operational policies, procedures, and guidelines, including manuals such as the *Oil and Gas Activity Application Manual*, see secondary 21100-00.

The agency OPR is the Applications Department, unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-01	**General**	CY+1y	nil	DE
-05	**Cancelled, expired, or refused applications** (covers applications which were approved, but no activities occurred so they were cancelled or expired without land disturbance, and applications which were refused) SO: when four years has elapsed since application approval with no activity occurring, or since refusal of the application NOTE: The retention provides time to cover the authorized two year permit period, a year for extension, and an extra year as a “grace period”, to discover if activity has actually occurred on the site. NOTE: This secondary applies to activity files (such as well files or pipeline project applications), which fit the criteria outlined above. NOTE: This secondary does not apply to declined or cancelled archaeological applications, which are classified under 20250-20.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20200 APPLICATION REVIEW

		A	SA	FD
-18	**Name changes, transfers and amalgamations** (covers name changes, transfers and company amalgamations for oil and gas activities such as wells, pipelines, facilities and roads) 12y: The twelve-year combined active and semi-active retention period is based on operational requirements to reference asset ownership history DE: Name changes, transfers, and amalgamations will be destroyed because the function and activities are sufficiently documented by BC Registries and Online Services.	CY+2y	10y	DE
-20	**Application files** (covers all permit and license applications received and approved by the Commission) (includes application forms, reviews, approval letters, permits, licenses, Indigenous consultation records, archaeological assessments, maps, mitigations, and other supporting documentation) SO: the application file will be considered closed when: • the permit or licence has expired, and for multi-authorization sites, all related permits and licences have expired; • permit conditions have been met; • and where relevant, the retention in the associated permitted activity file [i.e. well file] has expired • for archaeological permits, when no longer required to provide evidence of permitted archaeological activities SR: The government archives will selectively retain application files because they provide evidence of the use of land for activities that may have a significant long-term environmental impact. They document the Commission's comprehensive review of the applications for permits and authorizations. This includes the technical review of engineering, land and habitat, forestry, agriculture, archaeology, and environmental management, and the engagement process with Indigenous peoples, stakeholders, land owners and partner agencies. The records also	SO (cont.)	nil	SR

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20200 APPLICATION REVIEW

	A	SA	FD

-20 Application files (cont.)

document the decisions of the Commission, the permits and authorizations issues, the conditions imposed by the Commission for oil and gas development, and the rights and obligations of permit holders.

The records complement other records appraised for full retention: facilities (20600-30), pipeline projects (21000-35), well authorizations (21900-30) and reservoir analysis and management files (secondary 21400-35).

Applications for campsites, short-term use approvals (*Water Sustainability Regulation* (B.C. Reg. 94/2016), Part 4) and water notifications *(Water Sustainability Act*, (SBC 2014, c. 15, s.9) may be destroyed because these records relate to activities that have a minimal effect on the environment. All other types of application files will be fully retained.

NOTE: Permits and authorizations granted by the Commission include well, geothermal well, pipeline, facility, LNG facility, road, geophysical permits and all associated oil and gas authorizations including ancillary sites, investigative use, geotechnical investigation, aggregate operations, borrow pits, workspaces, campsites, water storage sites, changes in and about a stream, short-term water use and water licences. They also include non-farm use of lands in the Agricultural Land Reserve, master licences to cut, cutting permits, land tenure, waste management, archaeological investigation, inspection and alteration permissions, provincial authorizations related to pipelines subject to the *National Energy Board Act* and other miscellaneous oil and gas applications.

NOTE: The majority of permit applications are processed within the Application Management System (AMS). See the AMS System Overview for more information regarding application processes and contents.

(cont)

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20200 APPLICATION REVIEW

		A	SA	FD
-20	**Application files (cont.)** NOTE: Once an application is approved, an "activity file" is opened under the appropriate secondary for the following activities: Facilities 20600-30 Pipelines 21000-35 Roads 20900-30 Wells 21900-30			
-40	**Application review working files** (covers the working files of Commission staff who contribute to the application review process through consultation or technical reviews, such as archaeological, engineering, environmental, Indigenous, geological, or other reviews) (includes emails, notes, drafts and other material) SO: when no longer required for reference purposes, which is usually after application is approved and activity has commenced OPR: Oil and Gas Commission NOTE: This secondary includes permit-specific consultation with Indigenous peoples, which are currently managed in "e-binders". Non-permit specific records regarding Indigenous relations are classified under 20100-20. DE: The application review working files will be destroyed because the resulting decisions are documented in the application file (secondary 20200-20), which are selectively retained.	SO	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20250 ARCHAEOLOGICAL ACTIVITY MONITORING

Records relating to archaeological activities and the monitoring of permits issued under sections 12 and 14 of the *Heritage Conservation Act* (RSBC 1996, c. 187) (*HCA*).

Archaeologists working in British Columbia to excavate or alter the land for archaeological research or search for artifacts must have a permit, issued under the *HCA*, s. 14. The permit allows a qualified and permitted archaeologist to search for evidence of the existence of a site, authorize the systematic recovery of data from sites for research or mitigate the potential loss of data from the development of an area. Alteration permits, issued under *HCA*, s. 12, allow alterations in order to facilitate development of an area.

The Commission issues and manages these permits when they relate to oil and gas activities, on behalf of Forests, Land, and Natural Resource Operations and Rural Development (FLNROD).

Those permit files are classified under primary 20200 Application Review in this *ORCS*; this primary covers the related records to the issuance and monitoring of the permitted functions. Included in this primary is tracking information regarding the classification of archaeological sites, through Borden numbers, and the refused, cancelled or withdrawn applications. Also covered are final archaeological reports submitted as a requirement for s.14 permits, which are maintained as a reference collection. These reports summarize the activities completed by an archaeologist over the duration of their permit, and describe the activities outlined above.

For alteration permits (s.12), see secondary 20200-20.
For application review working files, see secondary 20200-40.
For archaeological audits, see primary 20550.
For operational policy and procedures, see secondary 21100-00.
For pre-application issues, see secondary 21600-25.
For s. 14 permits, see secondary 20200-20.
For tracking sheets and lists, see *ARCS* secondary 100-05.

The agency OPR is the Heritage Conservation Program, unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE
-05	**Borden numbers** (covers the temporary and permanent registration information for Borden numbers for BC sites; Borden numbers are the standard alpha-numeric naming convention for archaeological sites)	CY+1y (cont)	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20250 ARCHAEOLOGICAL ACTIVITY MONITORING

			A	SA	FD
		NOTE: Borden numbers are registered with the FLNROD Archaeology Branch; the retention allows time for lags in registration periods and tracking the numbers assigned to sites.			
	-10	**Final archaeological reports** (covers final reports submitted by archaeologists conducting work in the oil and gas sector, such as Archaeological Impact Assessments and site reports) SO: when no longer useful for reference purposes NOTE: These reports are initially used to reconcile permit conditions and ensure the documentation of archaeological activities and findings are complete. The set of reports have continued usefulness for reference, because they document archaeology sites and heritage inspection/investigation activities. DE: Final archaeological permit reports will be destroyed because they are maintained by the Archaeology Branch under secondary 11200-03 in the *Archaeology ORCS*, schedule 170415, where they are designated for full retention by the government archives. Reports or assessments related to a single application are copied to the relevant application file under 20200-20, which is fully retained by the government archives.	SO	nil	DE
	-20	**Declined, cancelled or withdrawn archaeological permits** (covers the background and rationale for the decision to decline, cancel or withdraw the application) SO: when no longer required for reference when reviewing subsequent archaeological applications NOTE: These records have long term reference value, as the reason or rationale for the decision can endure over time. The information documented in these files is relevant if a future application is received for the same site, and contributes to the Commission's collection of archaeological information. which have long term reference value, as the reason or rationale for those actions can endure over time	SO	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20300 COMPLIANCE AND ENFORCEMENT

Records relating to ensuring permitted oil and gas activities are conducted in compliance with the *Oil and Gas Activities Act* (SBC 2008, c. 36) (*OGAA*), related regulations, specified enactments and other applicable legislation.

This function is carried out through inspections and investigations, which may be triggered internally through routine inspection cycles, or from external sources, such as an incident or complaint. A complaint usually comes from the public regarding impacts potentially caused by an oil and gas activity, or non-compliance. The Commission evaluates and responds to those that are associated with an oil and gas permit holder with respect to their regulatory requirements or permit conditions. This includes maintenance of lease sites, ground disturbances, vegetation management, impact on waterways, use and maintenance of oil and gas roads, safe operations of wells, pipelines and facilities, odours, spills, or any similar concerns that have the potential to impact health, safety or the environment.

The compliance function is performed through the monitoring and inspection of permit holder activities, and investigation and enforcement of alleged non-compliance. The enforcement process encompasses tools and actions that work to keep activities and operations in compliance with legislation, including the issuance of orders, findings of contravention, and execution of administrative penalties, per the *Administrative Penalties Regulation* (B.C. Reg. 35/2011).

The Commission may issue orders with respect to activities and obligations under the Act. Orders are not contingent on a finding of contravention; they may also be issued if a person fails to comply with the Act, regulations, the person's permit or authorizations, or a previous order. Orders may also be necessary to mitigate a risk to public safety, protect the environment, or to promote the conservation of petroleum and natural resources. They specify whatever action must be taken, stopped or modified by the permit holder and includes the date by which they must comply. The Commission monitors compliance with the order.

The Commission may pursue further enforcement actions through a contravention decision if the permit holder does not comply with order requirements by the date specified, or if the alleged compliance issue is too significant to manage via an order. In this case, a Commission investigator develops a Contravention Report, containing detailed evidence outlining the permit holder's alleged contravention. The permit holder is given written notice of opportunity to be heard, in order to present the Commission with evidence supporting their defense.

At the end of the response period, the statutory decision maker will make a determination. The determination will indicate whether the permit holder is found in contravention of their obligations, and whether an administrative penalty will be imposed.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

For a description of the Integrated Resource Information System (IRIS), and Knowledge, Enterprise, Resource, Management, Information, and Technology (KERMIT), see the Systems Section.
For a list of classifications removed from this primary, see *Appendix A: Summary of Amendments to the OGCO ORCS.*
For legal matters, see *ARCS* primary 350.
For notebooks, see secondary 20000-06.
For reference material/topical files, see *ARCS* secondary 358-20.
For the Case File Ledger, see *ARCS* secondary 100-05.
For the *Compliance and Enforcement Manual*, deficiencies code list, Project Inspection Procedure form, and other operational policy or procedures, see secondary 21000-00.
For tracking spreadsheets, such as the Case File Ledger, see *ARCS* secondary 100-05.

The agency OPR is the Compliance and Enforcement Branch unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE
-05	**Complaints** (covers complaints in the KERMIT system) SO: when complaint is closed by being referred to another jurisdiction, determined to be unfounded/no action required, or resolved, and when no longer required for statistical reporting and trend analysis DE: Records in secondary 20300-05 will be destroyed because the compliance and enforcement function is sufficiently documented in the legislation, annual activity reports, policy and procedures, and orders and contravention decisions, all of which are designated for full retention by the government archives. NOTE: Complaints are managed in the KERMIT. When a complaint triggers an inspection or investigation the original complaint stays in the system, and there is a link to the related activities. NOTE: Complaints may originally come in through Emergency Management BC emails, which are scheduled under 20750-07.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20300 COMPLIANCE AND ENFORCEMENT

			A	SA	FD
	-40	**Enforcement case files** (covers all investigations into alleged non-compliance with regulatory and permitted requirements; commonly called case files, the outcome of these investigations may be that: the allegations are unfounded; the company is in compliance; or an enforcement action such as an order, a ticket, a warning or contravention decision) (includes investigation and continuation reports, background material such as notes, maps, photos, call logs and correspondence, and copies of administrative enforcement actions) (arrange by case file number) 15y: The retention ensures that the case file is available when establishing administrative penalties, and that it remains available while associated contravention decisions and orders are open. DE: Records in secondary 20300-40 will be destroyed because the compliance and enforcement function is sufficiently documented in the legislation, annual activity reports, policy and procedures, and orders and contravention decisions, all of which are designated for full retention by the government archives. NOTE: Investigations which result in an enforcement action may include the issuance of a formal investigation report, order, or contravention. Copies of those documents will be in these investigation files, but for original orders, see -65, and for contravention decision files, see -60.	CY+14y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20300 COMPLIANCE AND ENFORCEMENT

		A	SA	FD
-45	**Compliance issue and topic files** (sometimes called "non-enforcement files", this secondary covers collections of material from various sources, including other areas of the Commission, on topics which pertain to general compliance issues, and are useful for referencing in future inspections or investigations) SO: when reference value has expired DE: Records in secondary 20300-45 will be destroyed because the compliance and enforcement function is sufficiently documented in the legislation, annual activity reports, policy and procedures, and orders and contravention decisions, all of which are designated for full retention by the government archives. NOTE: Material relevant to a specific investigation or inspection is filed under the appropriate file (-40 and -50); this secondary may include copies of that material as part of the topical information (i.e. photos or notes).	SO	nil	DE
-50	**Compliance site inspections** (covers site inspections of wells, pipelines, facilities, roads, bridges, dams, crossings, rigs, etc., some of which are tied to an activity, and some "general" and associated with a company) (includes inspection preparation material, reports, deficiencies, deficiency responses, remedial actions, notifications and correspondence) SO: for inspections associated with a permitted activity, when the retention period for the activity (such as a well authorization) has expired; for general inspections not associated with a permitted activity, when 10 years have elapsed since remediation actions were completed DE: Records in secondary 20300-50 will be destroyed because the compliance and enforcement function is sufficiently documented in the legislation, annual activity reports, policy and procedures, and orders and contravention decisions, all of which are designated for full retention by the government archives. NOTE: The retention period ensures that access to the compliance history for permitted activities and the companies performing them is available.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20300 COMPLIANCE AND ENFORCEMENT

		A	SA	FD
-60	**Contravention decisions** (covers the decision for administrative findings of contravention, per *Administrative Penalties Regulation* (B.C. Reg. 35/2011)) (includes contravention report, opportunity to be heard hearing material, company response, correspondence, legal review and final decision) SO: when administrative penalties have been paid, and the review and appeal period has expired 10y: The retention period provides time to access a company's compliance history, which is a consideration when deciding on administrative penalties. FR: Contravention decisions and Orders will be fully retained because they provide evidence of the Commission's monitoring, inspection, investigation and enforcement of permit holder activities and alleged non-compliance with the *Oil and Gas Activities Act*, related regulations, specified enactments and other applicable legislation.	SO+10y	nil	FR
-65	**Orders** (covers orders issued to enforce a company's compliance with legislation and regulation, mitigate risk to public safety, protect the environment, or to promote the conservation of petroleum and natural gas resources) (includes background material, legal advice, the order, any amendments, the termination, and may include follow up confirmation of compliance) SO: when the conditions of the order have been satisfied, and the review and appeal period has expired (if relevant) 10y: The retention provides time to access a company's compliance history, which is a consideration when deciding on administrative penalties. OPR: Oil and Gas Commission	SO+10y	nil	FR

(cont)

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20300 COMPLIANCE AND ENFORCEMENT

	A	SA	FD

-65 Orders (cont)

FR: Contravention decisions and Orders will be fully retained because they provide evidence of the Commission's monitoring, inspection, investigation and enforcement of permit holder activities and alleged non-compliance with the *Oil and Gas Activities Act*, related regulations, specified enactments and other applicable legislation.

NOTE: Orders are issued under various acts, and are not always the result of a compliance investigation. Examples of other types of orders are OGAA s. 38 orders, which require a company to prepare, maintain and submit documents; s. 30 orders, which require a company to submit a security to ensure the performance of an obligation under the *Act*, permit or an authorization; or s. 50 action orders which allow the Commission to carry out an action referred to in the order. This secondary applies to all orders issued by the Commission, with the exception of orders relating to reservoir management, under s.75, which are filed under 21400-35.

NOTE: Records relating to compliance with the order are filed in the associated investigation file.

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20550 EXTERNAL AUDIT AND COMPLIANCE ASSESSMENT

Records relating to the Commission's audit programs, which evaluate, through a systematic and documented process, a permit holder's activities or programs and /or management systems against established criteria. For instance, evaluating a permit holder's compliance with regulatory requirements to have safety, management and procedural plans in place; or focus on a company's management system, including how the system is working in the field.

Examples of current external auditing programs performed by the Commission:

- Integrity Management Program Compliance Assurance: mandated by regulation, Integrity Management Programs (IMPs) provide a systematic approach for assuring asset integrity throughout the entire life cycle of the asset. The IMP audits focus on determining that the permit holders have a fully developed and implemented Integrity Management Program (IMP) that adheres to the requirements of the Canadian Standards Association, such as the CSA Z662 standard for Oil and Gas Pipelines Systems.

- Archaeological Audit Program: this program ensures client management systems are in place to support compliance with legislative, regulatory and permit obligations, and gathers baseline data to establish best management practices for archaeology management within the oil and gas sector.

- Restoration Verification Audit Program (RVAP): the objective of this program is to determine that Certificate of Restoration (CoR) regulatory requirements are being met, and that contamination at reclaimed oil and gas sites is being addressed in accordance with provincial regulatory requirements.

For emergency response exercise evaluations, see secondary 20750-30.
For policy, procedures and guidelines, both internal and external, such as the *Restoration Verification Audit Program Procedure Manual*, see secondary 21100-00.
For program development, see *ARCS* 400.
For reference material/topical files, see *ARCS* secondary 358-20.
For review/evaluation of programs, see *ARCS* 400.

The agency OPR is the Oil and Gas Commission unless otherwise noted below.
See specific secondaries for OPR retention schedules.

	A	SA	FD
All non-OPR offices will retain these records for:	SO	nil	DE
-01 General	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20550 EXTERNAL AUDIT AND COMPLIANCE ASSESSMENT

			A	SA	FD
	-10	**Final audit reports** (covers final audit reports, produced specifically for the company/audit project, and associated technical/scientific/lab data reports [for the RVAP audits]) SO: when no longer required for tracking a company's overall history of compliance with their regulatory requirements NOTE: Classify program reports produced on an annual basis, such as the cumulative Archaeological Audit Report, under 21600-30.	SO	nil	DE
	-20	**Audit working files** (includes research, correspondence, maps, site forms, checklists, tracking sheets, notifications, transcriptions, interview notes, self-assessment and supporting documents from the company, draft reports, copies of final reports, corrective action plans and follow-up) 10y: The retention ensures that the working file is available for reference in subsequent audits, and also ensures that the budget and invoicing material in the RVAP files are available for fiscal accountability. NOTE: Classify final audit reports under -10.	CY+10y	nil	DE
		DE: Final audit reports and audit working files will be destroyed because the audit framework is retained under 21600-00 Policy and procedures, and the annual reports that summarize audit implementation, processes involved in assigning ratings, audit results and recommendations for improvement, are retained under 21600-20, which is designated for full retention by the government archives. Also, final assessment reports and working files relating to the restoration of exploration and production sites will be destroyed because final assessment reports and the associated technical data are copied to the relevant well authorization file (21900-30), which is fully retained by the government archives.			

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20600 FACILITIES REGULATION AND MONITORING

Records relating to the ongoing monitoring of gas processing plants, production facilities and any other surface equipment deemed by the *Oil and Gas Activities Act (OGAA)* (SBC 2008, C. 36) to be a facility. *OGAA* defines a facility as "a system of vessels, piping, valves, tanks and other equipment used to gather, process, measure, store or dispose of petroleum, natural gas, water or substance." For example, gas processing plants are designed primarily for the extraction from natural gas of hydrogen sulphide, carbon dioxide, helium, ethane, natural gas liquids or other substances. A production facility is designed primarily to accommodate production or disposal or both production and disposal of well effluent products and byproducts.

The Commission monitors and regulates construction, modification and operation of all facilities, ensuring they meet the design and operational requirements outlined in the *OGAA, Oil and Gas Waste Regulation (OGWR)* (B.C. Reg. 254/2005), *Drilling and Production Regulation (DPR)* (B.C. Reg. 282/2010), the *Environmental Protection and Management Regulation (EPMR)* (B.C. Reg. 200/2010) and the *Liquefied Natural Gas Facility Regulation (LNGFR)* (B.C. Reg. 146/2014).

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS*.
For emergency response plans, see primary 20750.
For facility applications that are cancelled or expire without land disturbance, see 20200-05.
For facility applications, see primary 20200.
For facility Integrity Management Plan (IMP) compliance assessments, see primary 20550.
For operational policy, such as the *Oil and Gas Activity Operations Manual*, see secondary 21100-00.
For pipeline projects, see primary 21000.
For reference material/topical files, see *ARCS* secondary 358-20.
For wells, see primary 21900.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20600 FACILITIES REGULATION AND MONITORING

			A	SA	FD
	-30	**Facility files** (covers facilities such as gas plants, Liquid Natural Gas (LNG) facilities, refineries, dehydrator stations or compressor stations) (includes forms, specifications, schematics, drawings, testing, analyses, exemptions, construction plans, system diagrams, inspection reports and permits) (arrange by facility number) SO: when the facility has been removed, the site has been restored, and the file is no longer required to document activities conducted on the site NOTE: While a facility may be removed from a site, there is often sub-surface infrastructure (such as cut off pilings) remaining on site; these files document both the infrastructure and activity information. FR = The government archives will fully retain facilities records because they provide evidence of the use of land for activities that may have a significant long-term environmental effect. In addition, they document the rights and obligations of the permit holders in regards to gas processing plants and production facilities and the Commission's statutory responsibilities concerning the monitoring and inspection of these plants and facilities. The records also provide information about the ongoing evolution of oil and gas production in British Columbia; the management of the province's oil and gas resources; and government priorities regarding environmental protection, sustainable resource development, public and worker health and safety, cultural heritage, and Indigenous relations. The records complement the related facility permit applications, which are fully retained under secondary 20100-20.	SO	nil	FR

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20750 INCIDENT AND EMERGENCY RESPONSE

Records relating to the Commissions' response to incidents, per the *Oil and Gas Activities Act* (SBC 2008, c. 36) (*OGAA*) and the *Emergency Management Regulation* (B.C. Reg. 204/2013) (*EMR*).

During an oil and gas activity, an incident may occur that is outside of normal operations. Response includes the activities that address the short-term, direct effects of an incident. Depending on the magnitude of the incident, response may also include the execution of emergency plans.

Per the *EMR*, a permit holder is required to prepare and maintain an emergency response program and an emergency response contingency plan (or plans). The objective is to protect people, property and the environment by establishing a framework for emergency preparedness, planning and response. This is supported in the Commission by:

- Reviewing industry emergency management programs and plans.
- Evaluating permit holder emergency response exercises.
- Administering incident and complaint response processes.
- Leading emergency and incident follow-up and investigation.

Permit holders are the primary responders when incidents occur; they evaluate the situation, and take appropriate actions based on the nature and magnitude of the incident.

All emergency level incidents are reported through Emergency Management BC (EMBC). EMBC provides notification to the Commission, including a direct call to the emergency officer (EO.) The EO then contacts the permit holder, evaluates the situation, determines the appropriate actions and notifications, and will act accordingly. The Commission provides oversight and monitors events during incident and emergency response, and may direct additional resources to respond to any incident, or in rare cases, assume overall management of the incident.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For external audits, see primary 20550.
For external communications, such as safety advisories, see secondary 21600-06.
For inspections and investigations, see primary 20300.
For ledgers and tracking spreadsheets, see *ARCS* secondary 100-05.
For memoranda of understanding, such as with the National Energy Board, see *ARCS* primary 146.
For mutual aid agreements, see *ARCS* primary 146.
For operational policy and procedures, such as the *Emergency Management Manual*, or the exercise evaluation audit checklist, see secondary 21100-00.
For seasonal briefings, and other liaison with the emergency community, see *ARCS* secondary 230-20.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20750 INCIDENT AND EMERGENCY RESPONSE

		A	SA	FD
	The agency OPR is the Security & Emergency Management Branch, unless otherwise noted below. See specific secondaries for OPR retention schedules.			
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE
-05	**Company correspondence** (covers correspondence, commonly called letters, regarding timelines for exercises, approvals / amendments for emergency response plans, and variances for regulatory requirements) 10y: The retention ensures the correspondence is retained for a similar period as the associated exercises and emergency response plans, and that the company's compliance / activity information is available in support of determining administrative penalties.	CY+9y	nil	DE
-07	**Emergency Management BC reports** (covers the full set of emails, commonly called Dangerous Goods Incident Reports (DGIR's) or General Incident Reports (GIR's) which document all reported incidents that appear to be related to the oil and gas industry) NOTE: Complaints and incidents are manually entered into the KERMIT system, where they are managed as follows: incident reports which warrant a response are classified under -45 Incidents, and complaints and investigations under primary 20300.	CY+1y	nil	DE
-20	**Emergency response plans (ERP's)** (includes plans, checklist, correspondence) (arrange by company name) SO: when there have been three subsequent plans received, or when the asset that the supplemental plan relates to has had a certificate of restoration issued or remedial actions completed NOTE: The retention ensures the Commission will have the current plus two previous plans, for compliance support, and trend tracking. It also ensures that the plans for an orphaned well are available for the reclamation process.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20750 INCIDENT AND EMERGENCY RESPONSE

		A	SA	FD
-20	**Emergency response plans (ERP's)** (cont) NOTE: An ERP has two components: a core plan, which holds basic information about the company and its emergency policies that are not site-specific, and supplemental plans, which contain site specific information and plans for appropriate response. Currently, the Commission receives both an electronic and a hard copy of the ERP. The most recent hard copy is held for convenience purposes, as it is easily transportable in case of an emergency and for field work. However, it is a duplicate of the electronic ERP, and may be destroyed when replaced by an updated version, under the authority of special schedule 102901 (*Transitory Records*).			
-30	**Exercise evaluations** (covers the evaluation of a company's emergency response exercises, which test the emergency response program and the plan, and confirms that emergency response personnel know their duties) (arrange by company name) (includes notes, evaluation checklist and report, and follow up correspondence) SO: when no longer required to monitor whether a company is meeting response objectives and commitments; this will usually be two exercise cycles (6 years), and include at a minimum two full scale exercises NOTE: Permit holders usually perform emergency response exercises on a three-year cycle: two annual "table-top" exercises, followed by a full-scale functional exercise.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20750 INCIDENT AND EMERGENCY RESPONSE

			A	SA	FD
	-45	**Incident files** (covers minor incidents and lower level emergencies that are the result of an oil and gas activity; these may be spills, equipment failures or small fires) (includes reports and correspondence) (arrange by incident number) SO: when the incident and follow up activities are complete, and the information is no longer relevant for site reclamation OPR: Oil and Gas Commission DE: Incident files may be destroyed because major incident responses are fully retained under secondary 20750-50. In addition, information about incidents involving a fatality will be fully retained in Coroner's investigations case files (schedule 116356) and Commission guidance to industry about emergency planning, response and Emergency Response Plan requirements is fully retained under secondary 21100-00. NOTE: Because most incidents are spills, incident information is highly relevant to the reclamation of a site. Part of the reclamation process is assessing potential contaminants on the site by reviewing historical activities, spills etc. Incident information ultimately supports due diligence in addressing outstanding environmental concerns and helps to ensure sites are properly restored. NOTE: Classify major incidents, that potentially affect life and safety, warrant full investigation, or are managed through the Emergency Operations Centre (EOC) under -50.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20750 INCIDENT AND EMERGENCY RESPONSE

		A	SA	FD
-50	**Major incident and emergency response files** (covers incidents that may potentially affect life and safety, warrant full investigation, or are managed through the Emergency Operations Centre [EOC]) (includes notebooks, correspondence, shape files, and reports) (arrange by incident, and if managed through the EOC, then by role, such as incident commander, planning, operations, logistics, and finance & administration)	SO	nil	FR

SO: when the incident and follow up activities are complete, and the information is no longer relevant for site reclamation

OPR: Oil and Gas Commission

FR: The government archives will fully retain Major incident responses because they provide evidence of the Commission's responsibilities regarding the coordination, support, follow-up, and investigation of incidents and accidents that are significant due to their location or the nature of the incident and the potential effect on people and the environment. Incident responses also provide evidence of the collaboration that occurs within the Commission, between the Commission and other agencies or government bodies, and between the Commission and permit holder to ensure public and environmental safety.

NOTE: Because most incidents are spills, incident information is highly relevant to the reclamation of a site. Part of the reclamation process is assessing potential contaminants on the site by reviewing historical activities, spills etc. Incident information ultimately supports due diligence in addressing outstanding environmental concerns and helps to ensure sites are properly restored.

NOTE: Classify minor incidents under -45.

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20850 LIABILITY MANAGEMENT

Records relating to the management of liability with regards to oil and gas assets, through the Liability Management Rating (LMR) program and orphan site management.

The intent of the LMR program is to identify permit holders whose estimated oil and gas decommissioning liabilities exceed their estimated oil and gas assets. In such cases, the identified permit holders are required to take steps to address the financial risk related to their operations. The LMR program enables the Commission to determine security deposit requirements of the permit holders as a protection measure, in the event they are not capable of meeting abandonment and reclamation obligations.

This primary also covers orphan site management. Under the *Oil and Gas Activities Act* (SBC 2008, c. 36) (*OGAA)*, the Commissioner can designate orphan sites (a well, facility, pipeline and/or area affected by oil and gas activity) when a regulated permit holder cannot be located or is insolvent. Before the Commissioner designates an orphan site, the Commission exhausts every possibility to ensure those responsible, even in bankruptcy, are held financially accountable. When an orphan site is designated, the Commission may use the Orphan Site Reclamation Fund (OSRF) to decommission and restore the site. The restoration process provides assurance to stakeholders that oil and gas infrastructure has been removed, and that all known contamination risks or other hazards have been mitigated.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For annual LMR Summary reports, see secondary 21600-20.
For policy and procedures, such as the *LMR Program Manual*, see secondary 21100-00.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

	A	SA	FD
All non-OPR offices will retain these records for:	SO	nil	DE
-01 General	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20850 LIABILITY MANAGEMENT

		A	SA	FD
-03	**Security deposit files** (covers the liability calculation files for both drilling deposits, created under the *Petroleum And Natural Gas Act*, RSBC 1996, C. 361, S. 160, and security deposits, created under the *Oil And Gas Activities Act,* SBC 2008, C. 36, S. 30 and pursuant to the *Fee, Levy and Security Regulation*, (B.C. Reg. 8/2014)) (includes security drilling deposit requirements for companies, cost estimates, correspondence, financial statements and reviews) SO: when the security has been returned to the company, or transferred to another operator or the Orphan Site Reclamation Fund 10y: The retention period allows for fiscal accountability and aligns with Board policy which allows 10 years to reclaim an orphan well. NOTE: The Commission may return security deposits to the permit holder when they have achieved a consistent and sustainable liability rating, and have demonstrated compliance with regulatory obligations, or when they no longer hold assets in the province. If the related asset(s) become an orphaned site, the security will be transferred to the OSRF.	SO+1y	9y	DE
-20	**Corporate asset files for orphaned or at-risk sites** (covers corporate asset files received from insolvent or at-risk companies whose assets have either been designated as orphaned, or may potentially be orphaned. The Commission receives these files to support the future transfer of the asset to a responsible party and prevent the site from being orphaned, or in the interest of having all information possible to assist in the restoration of the orphaned site) SO: when no longer useful to support the transfer of the site or the restoration of the orphaned site DE: These records may be destroyed because records relating to the Commission's permit and licence approvals and the monitoring and regulating of oil and gas activities are fully retained under 20200-20, 20600-30, 20750-50, 20900-20, 21000-35, 21400-35 and 21900-30.	SO	nil	DE

(cont)

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20850 LIABILITY MANAGEMENT

		A	SA	FD
-20	**Corporate asset files for orphaned or at-risk sites (continued)** NOTE: If the Commission is successful in finding a company who will take on the management of the assets, the associated files may be transferred to the new responsible party. Those files are classified under -21 Corporate asset files for transferred assets.			
-21	**Corporate asset files for transferred assets** (covers corporate asset files which are being transferred to a responsible party to assist them in the ongoing management and eventual reclamation of the site) SO: when the ownership of the asset has been transferred to the responsible party / new permit holder NOTE: These files are originally created by oil and gas companies and transferred to the Commission because of their value in assisting with the transfer of the asset to another company for ongoing management. Many parts of the corporate file duplicate the Commission's files, and hold no value to the Commission, yet have great value to the receiving company so they may understand the operations and details of the assets they are acquiring. OD: These records may be transferred to a new permit holder so they can understand the operations and details of the assets that they are acquiring, and because records relating to the Commission's permit and licence approvals and the monitoring and regulating of oil and gas activities are fully retained under 20200-20, 20600-30, 20750-50, 20900-20, 21000-35, 21400-35 and 21900-30.	SO	nil	OD

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20900 ROAD REGULATION AND MONITORING

Records relating to permits for use of and access to roads as part of the infrastructure required for oil and gas activities such as wells, pipelines, and facilities. All permits are issued in accordance with the *Oil and Gas Road Regulation* (B.C. Reg. 56/2013) (*OGRR*), but this primary also covers roads or portions of a road originally authorized and constructed under the *Land Act* (RSBC 1996, c. 245) or the *Petroleum and Natural Gas Act* (RSBC 1996, C. 361), as a Petroleum Development Road. Authorization for the permit holder to make changes in or about a stream comes from the *Water Sustainability Act* (SBC 2104, c. 15).

There are a variety of types of oil and gas roads applicants may apply for, such as:

- Long-term, all-weather roads: roadbeds surfaced with gravel.
- Short-term, low-grade roads: constructed during non-frozen ground conditions.
- Snow and/or ice roads: activities carried out during frozen ground conditions with minimal soil disturbance.

The records in this primary document the road "activity file." Road permit holders have obligations regarding the construction, maintenance, use and deactivation of oil and gas roads, including clearing widths, bridges and culverts, hazard warnings and post-construction reporting.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS.*
For inspections, see secondary 21300-50.
For operational policy, see secondary 21100-00.
For road permit applications, see secondary 20200-20.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE
-20	**Road files** (formerly called Petroleum Development Roads (PDR's), this secondary covers the post-approval activity information for road permits, which approve the construction of roads, bridges and culverts for oil and gas activity) (includes maps, special studies, reports and notices, and for original PDR files, the applications)	SO+5y	nil	FR
	SO: when the road has been cancelled or deactivated, and restoration is complete	(cont)		

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20900 ROAD REGULATION AND MONITORING

		A	SA	FD
-20	**Road files (continued)**			
	5y: The retention provides time to ensure there are no issues with the deactivation, cancellation, or restoration of the road.			
	FR: The government archives will fully retain Road files because they provide evidence of the use of land for activities that may have a significant long-term environmental effect. They also provide information about the construction, maintenance, use and deactivation of oil and gas roads. The records complement the related road permit applications, which are fully retained under secondary 20200-20.			

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21000 PIPELINE REGULATION AND MONITORING

Records relating to the regulating and monitoring of all pipelines within the boundaries of the province which have been constructed or are operating under the jurisdiction of the government of British Columbia. The *Oil and Gas Activities Act* (*OGAA)* SBC 2008, c. 36) defines a pipeline as "piping through which any of the following is conveyed: petroleum or natural gas; water produced in relation to the production of petroleum or natural gas or conveyed to or from a facility for disposal into a pool or storage reservoir; solids; substances prescribed under section 133 (2) (v) of the *Petroleum and Natural Gas Act* (RSBC 1996, c. 361); other prescribed substances, and includes installations and facilities associated with the piping".

The Commission monitors the construction, modification and operation of all pipelines, ensuring they meet the design and operational requirements outlined in the *OGAA*, the *Pipeline Regulation* (B.C. Reg. 281/2010) and the *Environmental Protection and Management Regulation* (B.C. Reg. 200/2010). Of particular note, as required under Section 3 of the *Pipeline Regulation*, every permit holder designing, constructing, operating, maintaining or abandoning pipeline infrastructure in British Columbia must follow the most current version of CSA Z662, including Annex N.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS.*
For facilities, see primary 20600.
For operational policy, such as the *Oil and Gas Activity Operations Manual*, see secondary 21100-00.
For pipeline applications, see primary 20200.
For pipeline Integrity Management Plan (IMP) compliance assessments, see primary 20550.
For reference material/topical files, see *ARCS* secondary 358-20.
For wells, see primary 21900.

The agency OPR is the Oil and Gas Commission unless otherwise noted below.
See specific secondaries for OPR retention schedules.

	A	SA	FD
All non-OPR offices will retain these records for:	SO	nil	DE
-01 General	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21000 PIPELINE REGULATION AND MONITORING

		A	SA	FD
-35	**Pipeline projects** (includes forms, maps, drawings, specifications, exemptions, schematics, permits, testing results, analyses, correspondence, and photographs) (arrange by pipeline project number) SO: when the pipeline has been removed, or no longer exists NOTE: These records will be retained by the Commission for an indefinite period of time because pipelines are rarely removed from the ground after being cancelled, and even when parts are removed, sections which could be disruptive to the environment to take out (such as under a river) will remain underground. This lengthy retention period is required to document the activities and the locations of the lines. FR: The government archives will fully retain pipeline project records because they provide evidence of the use of land for activities that may have a significant long-term environmental effect. In addition, they document the rights and obligations of the permit holders in regards to pipeline construction and operation, and the Commission's statutory responsibilities concerning the monitoring of pipelines. The records also provide information about the ongoing evolution of the technical aspects of pipeline design and construction in British Columbia and the Commission's priorities regarding environmental protection, sustainable resource development, public and worker health and safety, cultural heritage, and Indigenous relations. These records complement the related permit applications, which are fully retained under secondary 20200-20.	SO	nil	FR

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21100 POLICY AND PROCEDURE DEVELOPMENT

Records relating to the development of operational guidelines and policies, including procedures, standards, protocols, recommended practices and directives, that are for internal use, and also for external use to assist clients, First Nations and stakeholders with clarification of operational requirements. The requirements are a resource tool for companies and provide direction to industry to ensure safe and efficient practices.

For committees, see *ARCS* secondary 200-20.
For fee and levy changes, see *ARCS* primary 140.
For legislation and regulation development, see *ARCS* primary 140.
For program planning, see *ARCS* secondary 400-20.
For reference material/topical files, see *ARCS* secondary 358-20.

The agency OPR is the Oil and Gas Commission unless otherwise noted below.
See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-00	**Policy and procedures - final** (covers final/approved policies, procedures, standards, protocols and guidelines pertaining to the functions and activities documented in this *ORCS,* and developed for internal or external use, including operational manuals such as the *Oil and Gas Activity Operations Manual*, the *Compendium*, and OGC process maps) (arrange by category if necessary, and then by policy name or registration number) SO: when the policy/procedure is replaced or becomes irrelevant; for policy/procedures which are required to provide point-in-time evidence, such as environmental and wildlife policy, when no longer needed to provide evidence for decisions FR: The government archives will fully retain final versions of operational policy and procedural documentation because they provide evidence of the governance of the functions and programs covered by this *ORCS*.	SO	5y	FR
-01	**General**	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21100 POLICY AND PROCEDURE DEVELOPMENT

			A	SA	FD
	-20	**Policy, guideline, and procedure development files** (includes briefing notes, correspondence, drafts, and working materials) SO: when the final product is approved and distributed, or abandoned, and when no longer required for reference DE: Policy, guidelines and procedure development files will be destroyed because final products are fully retained under secondary -00.	SO	5y	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21400 RESERVOIR REGULATION AND MONITORING

Records relating to the regulation and monitoring of petroleum and natural gas reservoirs in the province, and the subsurface storage or disposal of associated products or by-products. The Commission ensures compliance with requirements for wells, the allowable production of wells, and the development of effective and efficient engineering practices through the approval and monitoring of reservoir projects.

An example of a reservoir project includes storage of natural gas in depleted high porosity/permeability reservoirs to provide supply during peak demand periods. Traditionally, this means that gas injected in summer is withdrawn to meet winter heating requirements. Another project type is concurrent production, the controlled simultaneous production of an oil accumulation and its associated gas cap.

This primary also includes the records which map the oil and gas field and pool boundaries. These boundaries are outlines on the earth's surface that define a subsurface oil or gas accumulation.

For operational policy and procedures, see secondary 21100-00.
For reports produced on an annual basis, such as the *Hydrocarbon and By-product Reserves Report*, see 21600-20.

The agency OPR is the Field Engineering and Technical Services, unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	nil	DE
-25	**Geological topical files** (covers information regarding subsurface composition and contents, gathered for convenience and reference purposes) (arrange by field, formation or topic) SO: when no longer useful for reference purposes NOTE: This secondary covers a compilation of material gathered from outside sources, as well as material that is part of other Commission applications and files (i.e. well reclassification applications or geological maps, plats and cross-sections from field and pool applications that are classified under -35).	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21400 RESERVOIR REGULATION AND MONITORING

		A	SA	FD
-35	**Reservoir analysis and management** (commonly called field and pool files, this secondary covers projects that relate to managing and analysing reservoir contents; also covers records that document the reservoir properties, characteristics and boundaries) (arrange by field, then by pool, then by project type) (includes applications, analysis, approvals, orders, tests and reports for projects such as water disposal, good engineering practice (GEP), concurrent production, waterflood, gas reinjection, experimental/innovative technology, acid gas disposal, acid gas disposal progress reports, commingling, spacing and target areas, reservoir worksheets, initiating well testing waivers and observation wells, as well as field or pool net pay maps, designations and lists)	SO	nil	FR

SO: the files are closed according to the following criteria:

- for records relating to production management, such as Good Engineering Practices (GEPs), 20 years after pool abandonment;
- for records relating to projects that resulted in a changed subsurface environment or have potential safety considerations in future activities, such as disposals and waterflood projects, when no longer required to provide evidence of the activities;
- for records which document the composition and structure of the field or pools, when that information is no longer required.

FR: The government archives will fully retain Reservoir analysis and management files because they provide evidence of the use of land for activities that may have a significant long-term environmental effect. In addition, they document the rights and obligations of permit holders and the Commission's statutory responsibilities to ensure safe and effective reservoir management. The records also provide information about the ongoing evolution of engineering principles used to maximize resource recovery. The records complement other permit application and related oil and gas activity records, which are appraised for full retention under secondaries 20200-20 and 21900-30.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21400 RESERVOIR REGULATION AND MONITORING

			A	SA	FD
	-40	**Production allowable reports** (covers oil and gas allowable reports, which document managed production flows from oil and gas wells) (arrange by company, then by production year) SO: the end of the production year the report covers 7y: The retention ensures the information is available to track a company's compliance with their regulatory requirements and permitted production rates; support royalty calculations; and provide rationale for decisions made around changes to production rates. NOTE: The production year runs from November 1st to October 31st.	SO	7y	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21600 STAKEHOLDER RELATIONS

Records relating to communication with stakeholders involved in the development of the province's oil and gas sector. This includes informational communications regarding Commission directives, advisories and initiatives. It also includes consultation on matters related to rights, terms of entry on private and agricultural leased lands, and oil and gas activities, which provides an opportunity for public participation, identification of any issues or concerns, and education for affected parties about oil and gas development projects.

This primary also covers the communication of both sector and corporate performance. Corporate performance reports identify goals, objectives, performance measures, and other strategic information. Corporate performance objectives are formally communicated in service plans, and performance actuals in annual reports.

For news releases, see *ARCS* primary 330.
For policy and procedures, see secondary 21100-00.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-01	**General**	CY+1y	nil	DE
-03	**General inquiries**	CY+1y	2y	DE
-06	**External communications** (covers communication products such as information letters, industry bulletins, directives, safety advisories, fact sheets and other methods of communicating Commission information to external stakeholders) (includes drafts, correspondence, and final products) 10y: The retention provides sufficient time to reference the way the Commission addressed issues and communicated to stakeholders over time. It also aligns with special schedule 102906, *Executive Records*. NOTE: Classify reports produced on an annual basis (both technical and performance reports) under -20. FR: The government archives will fully retain External communications. They provide evidence of what information is conveyed by the Commission to clients, Indigenous peoples, communities and multiple levels of	CY+3y	6y	FR

(cont)

FR:	The government archives will fully retain External communications. They provide evidence of what information is conveyed by the Commission to clients, Indigenous peoples, communities and multiple levels of	(cont)

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21600 STAKEHOLDER RELATIONS

			A	SA	FD
	-06	**External communications (continued)** government about oil and gas operations and activities in British Columbia, and the methods and tools used to communicate that information. This is consistent with the full retention of communication projects in the *Government Communication ORCS* (schedule 881035, secondary 23100-30). The records also complement policies and procedures, which are appraised for full retention under secondary 21100-00.			
	-20	**Annual activity reports** (covers technical, analytical and performance reports created by the Commission on an annual basis that document both Commission and industry activities, such as the Hydrocarbon and By-Product Reserves in British Columbia, the Pipeline Performance Summary, the Annual Service Plan and others) (arrange chronologically by fiscal year) SO: when no longer being used for trend analysis, and understanding Commission and activity history NOTE: Classify report development under secondary -30 FR: The government archives will fully retain Annual activity reports because they provide evidence of the Commission's structure, activities, priorities, and finances.	SO	nil	FR
PIB	**-25**	**Pre-application issues case files** (covers issues and concerns that are raised at the pre-application stage of the permit process, such as landowner liaison issues, archaeological inquiries, or technical advice for the preparation of applications) (arrange by name of company or landowner) SO: when issue is resolved or no longer relevant, or the permit is approved and activity has commenced, and when no longer needed for reference and tracking purposes DE: Pre-application issues case files will be destroyed because the Commission's role in dispute resolution is well documented in Policy and procedures – final (secondary 21100-00) and the mitigation of issues is documented on the related Applications file (20200-20), which will be fully retained by the government archives.	SO	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21600 STAKEHOLDER RELATIONS

			A	SA	FD
	-30	**Report development files** (covers the development material for reports that are created on an annual basis) (arrange by report) SO: when report has been published, or abandoned, and when development material is no longer required for reference purposes NOTE: Classify final annual activity and service plan reports under -20.	SO	nil	DE
PIB	**-35**	**Stakeholder issues** (covers the resolution of issues and concerns that are not related to specific permits, applications, or part of the pre-application process) SO: when issue is resolved or no longer topical, and when no longer needed for reference purposes	SO	nil	DE
	-40	**Strategic engagement projects** (covers strategic projects regarding consultation or engagement plans) (arrange by project) SO: when project is completed, cancelled, or abandoned 7y: The retention period ensures that the records are available for a sufficient period for reference and program planning purposes. NOTE: Classify business planning and strategic planning for the Commission under *ARCS* primary 400. DE: Strategic engagement projects will be destroyed because sufficient information about these functions are documented in service plans and annual reports (secondary 21600-20) and application files (secondary 20200-20), which are fully retained by the government archives.	SO+7y	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21700 TIMBER CUTTING LICENSING

Records relating to the issuance, monitoring and administration of Master Licenses to Cut (MLTC), which are required where the removal of Crown timber is necessary to conduct oil and gas activities. The MLTC allows the company to cut and/or remove timber during the term of the license, from areas of Crown land that are located within a specified forest district; cutting permits are issued under the master license to authorize the cutting on specific individual blocks. All master licenses are issued pursuant to the *Oil and Gas Activities Act* (SBC 2008, c. 36) and the *Forest Act* (RSBC 1996, c. 157).

For a description of the Integrated Resource Information System (IRIS), see the Systems Section.
For operational policy, see secondary 21100-00.
For records relating to cutting permits, see primary 20200.

The agency OPR is the Applications Department, unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-01	**General**	CY+1y	nil	DE
-20	**Master licenses to cut** (arrange by company, then by master license number) SO: when replacement master license is issued, or license has expired DE: Master licenses to cut will be destroyed because they do not have long-term value. Individual cutting permits related to these licenses are filed on the appropriate application file (secondary 20200-20), which is fully retained by the government archives.	SO	nil	DE

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21900 WELL REGULATION AND MONITORING

Records relating to the technical information and analyses related to the potential for and methods of extracting petroleum, natural gas or other energy resources from specific wells. The Commission regulates and monitors the exploration and development of oil and gas activities, including the management, long term protection and conservation, control and treatment of wells. All data connected with or derived from drilling, production or other work performed on a well must be submitted to the Commission. Submission requirements include reports, surveys, testing and analyses, samples, cores and logs. The Commission must give approval for any changes, transfers or amendments made to a well authorization as well as issue associated certificates, permits, and authorizations.

Wells are classified according to criteria outlined in the *Drilling and Production Regulation* (B.C. Reg. 282/2010, s. 2); well reports and data are held confidential for the associated periods of time established in the *Oil and Gas Activities Act General Regulation* (B.C. Reg 274/2010, s. 17). After the confidential periods have expired, well information held by the Commission is routinely released. For example, wells classified as developmental are held confidential for two calendar months, after which the well data and well reports are available to industry and the public.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a description of the Integrated Resource Information System (IRIS), see the Systems Section.
For convenience copies, kept for administrative purposes and ease of reference, see special schedule 102901 (Transitory Records Schedule).
For facilities, see primary 20600.
For liability management, see primary 20850.
For operational policy, see secondary 21100-00.
For orphan wells, see primary 20850.
For pipelines, see primary 21000.
For security deposits, see secondary 20850-03.
For well applications, see primary 20200.
For well authorization applications that are cancelled or expire without land disturbance, see 20200-05.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

	A	SA	FD
All non-OPR offices will retain these records for:	SO	nil	DE
-01 General	CY+1y	nil	DE

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

21900 WELL REGULATION AND MONITORING

			A	SA	FD
	-30	**Well authorization files** (arrange by well authorization number) (includes well and test hole amendments, revisions, exemptions, title clearance sheets, drill stem test, applications and approvals (e.g., to alter or abandon a well, for allowable production), well summary reports, work-over and completion reports, geological reports, well site access and cleanup reports, certificates of restoration, correspondence, well name changes and transfers, well logs or formation evaluation logs)	SO	nil	FR

SO: when a certificate of restoration is issued and the well information is no longer needed for environmental and safety management

NOTE: These records will be retained for an indefinite period of time because the geological and technical well information holds long-term value for future exploration, as well as for managing the lifecycle of the well. Also, well integrity issues can arise long after a well is considered remediated or “closed”. In these situations, immediate access to the file is necessary to manage safety and environmental issues.

FR: The government archives will fully retain Well authorization files because they provide evidence of the use of land for activities that may have a significant long-term environmental effect. In addition, they document the rights and obligations of permit holders and the Commission’s statutory responsibilities to ensure safe and effective extraction of resources. The records also provide information about the ongoing evolution of the methods of extracting petroleum, natural gas, or other energy resources. The records complement other records appraised for full retention: applications (secondary 20200-20); facilities (20600-30), pipeline projects (21000-35), and reservoir analysis and management (secondary 21400-35).

END OF PRIMARY

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

OIL AND GAS REGULATION

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (*ORCS*)

SYSTEMS SECTION TABLE OF CONTENTS

SECTION AND TITLE	PAGE NO.
COMMON SYSTEM NOTES	2
Application Management System (AMS)	3
Integrated Resource Information System (IRIS)	8
Knowledge, Enterprise, Resource, Management, Information, and Technology (KERMIT)	11

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

SYSTEMS SECTION: COMMON SYSTEM NOTES

Retention Schedules for the Systems

The data on the systems are classified under appropriate secondaries in the *ORCS* and in *Administrative Records Classification System* (*ARCS*), as indicated in the following descriptions. The systems themselves are all scheduled as follows:

Active	SO:	The system becomes superseded and obsolete when all data have been migrated to another system or documented elsewhere, or when all applicable retention schedules for the data have expired; see relevant classifications.
Semi-Active	nil:	There is no semi-active retention period assigned to systems.
Final Disposition	DE:	Each system will be destroyed when all data has been migrated to a new system performing the same function, or when the function it supports is no longer performed by the provincial government, and when the approved retention schedules covering the information on it have elapsed, or the information has been preserved elsewhere. For more information, see DE appraisal notes under the secondaries that cover the data.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPLICATION MANAGEMENT SYSTEM (AMS)

SYSTEM OVERVIEW

Creating Agency
Oil and Gas Commission

Purpose and overview
The Application Management System (AMS) is an online system for the submission, payment, review and approval of the majority of oil and gas and associated activity applications received by the Commission. It provides a consistent process for oil and gas activity permit applications, related activity authorization applications, applications for provincial approvals for National Energy Board (NEB) pipelines, and holds historical data submissions.

The system has three modules: AMS Application, AMS Payment, and AMS Review.

AMS Application (also called ePermits)

Inputs
Application information depends on the type and location of the activity. The information collected regarding an application is organized by the following categories:

- Spatial data
- Administrative information
- Land
- Forestry
- Stewardship
- Agriculture
- Archaeology
- Consultation and notification
- Rights holder
- First Nations
- Maps and plans
- Attachments

Also documented in the application are activity details, which outline the planning, design and technical requirements. Additional supplementary information may be required depending on the type of oil and gas activity, location, and engineering and technical details provided.
Examples of activity details for type of application:

- Wells: well/facility application area spatial (WFAA), well details, and land information
- Facilities: WFAA spatial, facility overview, facility details including equipment details, technical specifications and exemptions; and land information
- Roads: road application area spatial (RAA),road type and overview, road details, and road land information
- Short-term water use: points of diversion spatial, overview and points of diversion details
- Pipeline: pipeline application area polygons (PAA), pipeline overview, pipeline details including segment linkages; installation details and exemptions; and land information
- Geophysical: geophysical details such as program type, energy source and construction method, and geophysical land information
- Associated Oil and Gas Activities (AOGA), such as access, above ground fresh water line, aggregate / borrow pits, airstrips, campsites, fresh water storage sites, monitoring sites: activity details and land information
- Changes in and about a stream: stream details, planning and design, and exemptions

The final record of an application file will hold the consultation, mitigation plans, conditions and technical details of the permitted activity.

Process

Application information is entered by or derived from data submitted by the applicant. Attachments are uploaded directly. The online application submission process includes:

- Using the Application Analysis Tool (not mandatory)
- Reviewing the dashboard
- Creating a new application
- Uploading spatial data
- Completing, validating, and submitting the application.

Applicants can either start building their application directly, or test/build the application using the "Application Analysis Tool" provided.

If the client chooses to use the Application Analysis Tool, they have the capability to submit their spatial data and run a Spatial Overlay Engine (SOE) report. This report will identify known environmental, social and land considerations, such as highlight areas overlapping the surface location of the proposed activity, including tenures, land and resource planning zones, and areas established by order. Applicants can use this information to plan engagement activities (notification and consultation) and/or mitigation strategies, and allows applications to pinpoint the best location for a project at the beginning of the process. Using this tool will not generate any activity identifiers. If the user so choses, they can directly move this data into an official application submission (they cannot start an amendment in this fashion at this time).

AMS is the system of records for the majority of applications to the Commission. Once an application is approved and the permit issued, additional material cannot be added to it.

AMS Payment (also called ePayment):

Application fees must be paid by companies who have submitted applications to the Commission for oil and gas activity permits. Application fees are transferred to the Commission via electronic funds transfer (EFT) through the Application Management System (AMS) payment module. AMS Payment is the secure, online portal used to electronically pay for applications submitted through the AMS using Pre-Authorized Debit. Applicants are required to register and set up security roles for a secure payment account with AMS Payment.

Process:
Invoices for new AMS applications of type 'Application" are automatically generated on the dashboard on the basis of the:

- Activity information for the application
- Inventory codes for each activity

Invoices for AMS applications of type 'Amendment', and manual payments (not associated with AMS activities) are generated manually by finance staff based on:

- Activity information for the amendment
- Inventory codes for each activity according to the activity and information provided by reviewers through a manual process.

Only users with Payor permissions can pay for an invoice. Invoices are paid through the ePay dashboard using the authorization code and EFT set up in ePayment

Outputs
Invoices are the sole output of AMS Payment. These can be downloaded as .PDF documents from within the ePayment application.

AMS Review (also called Categorization and Review Determination [CRD]):

All review and determination data is recorded in this application. This includes the multiple review type recommendations, and the final decision and rationale. There can be many attachments included with each application review in support of any of the recommendations or the decision. In the case of a partial or full approval, a permit will also be attached to the record. AMS is the system of record for the majority of applications to the Commission. Once an application is approved and the permit issued, additional material cannot be added to it.

Process
Applications submitted through AMS Application are moved into the AMS Review system. The Commission conducts a comprehensive technical review of the application based on the characteristics, location and circumstances of the activity. Technical reviews include engineering (facilities, pipelines or drilling and production), land and habitat, forestry, agriculture, archaeology and environmental management.

During this review and determination process, the Commission also conducts a wide range of engagement processes, liaising with Indigenous peoples, stakeholders, land owners and partner agencies. If the Commission finds minor and/or major deficiencies in the application, the Commission contacts the applicant to clarify details, make revisions and/or provide additional information.

Based on activity types and location, the system assigns specific reviews types or tasks to appropriate staff for completion. These include the following:

- Historical Pipeline Land Review
- Historical Pipeline Engineering Review
- Historical Facility Review
- Commission Initiated Amendment Determination
- CIA Post Decision Tasks
- First Nations
- Land and Habitat
- Forestry
- Agriculture
- Consultation and Notification
- Composite Application
- Pipeline Engineering
- Facility Engineering
- Drilling and Petroleum Engineering
- Community Relations
- Archaeology
- Environmental Management
- Hydrogeology
- Post Decision Tasks

Details from the review and engagement processes are recorded in the CRD database by the AMS Review system.

The permit decision maker ensures that all aspects of an application – indigenous, archeological, landowner and community liaison, environmental, land, geology and technical are reviewed and signed off by the appropriate commission staff before approving and issuing the permit.

Once an application is approved, the associated data is moved to the operational databases and made available to the Commission's operational systems. The approved activities are available in KERMIT and IRIS for the ongoing collection of information.

Outputs
The main outputs of AMS system are approved activities and Permit documents. Permit documents are manually created by Commission staff and attached to the CRD review and determination record manually.

Historical Note
AMS was implemented in July 2016, and replaced a paper-based process in which staff provided all application analysis and processing.

Previous to AMS, pipeline applications were submitted to KERMIT. The KERMIT database is still operational and is now the system of record for "pipeline activity files", among other activities. Pipeline applications are now submitted through AMS.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPLICATION MANAGEMENT SYSTEM (AMS)

Classifications of Records that Relate to the System

Schedule Code	Secondary No.	Secondary Title	Retention Schedule A	SA	FD
Data in the System					
OGCO	20200-05	Cancelled, expired or refused applications	SO	nil	DE
OGCO	20200-20	Application files	SO	nil	SR
Inputs					
OGCO	20200-40	Application review working files	SO	nil	DE
Other Related Records					
ARCS	6820-05	Back-up data	SO	nil	DE
ARCS Section 6	see appropriate secondaries	INFORMATION TECHNOLOGY			
102902		Special Schedule for Transitory Electronic Data Processing (EDP) Records	SO	nil	DE

Schedule Code Key: *ARCS = Administrative Records Classification System,* schedule 100001
OGCO = Oil and Gas Regulation ORCS, schedule 163507

END OF OVERVIEW

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

INTEGRATED RESOURCE INFORMATION SYSTEMS (IRIS)

SYSTEM OVERVIEW

Creating Agency
Oil and Gas Commission

Purpose
The purpose of the Integrated Resource Information System is to track and maintain a database of all oil and gas related development from its initial proposal to its approval, eventual project completion and continuous monitoring and inspection.

Information Content
IRIS is the operational management system for wells, roads, geophysical, associated activity and Changes In and About a Stream (CIAS) operational activities. The information in IRIS relates to all aspects of operational data for well engineering/production data

Inputs, Processes, and Outputs

Inputs
Information is entered into IRIS in multiple ways:

- Application Management System (AMS): Approved activities are moved from AMS Application into a database, which IRIS reads and presents the data directly in its screen
- eSubmission: Operational data is submitted by companies through the external eSubmission portal; this includes information such as drilling and workover submissions, water user reporting, and various other submissions.
- Data Load: Data is imported from external systems.
- Manual Data Entry: Some operational data is entered into IRIS by Commission staff.

Processes

IRIS provides the following core functionality, by activity type:

- Wells: Provides summary views of all approval and operational data such as well status, subsurface activity and reported data and associated processes. Additional information associated with operational wells is available/managed in IRIS:
  - Drilling
  - Production
  - Waste Disposal
  - Geology
  - Reserves (reporting and Pay Zone maintenance)
- Geophysical: holds approved activity data, and provides summary and required reporting.
- Roads: holds summary activity data for each road and its associated activities. Road specific reporting is also provided.
- Associated Activities: summary reporting and operational views of associated activities.
- CIAS: summary reporting.
- Water Use: reporting.

Additional functionality is also provided for with legacy (pre AMS) application data, legacy Pipeline data, and some limited inspection functionality (specifically Surface Case Vent Flow functionality).

Outputs

- Reports.
- Outputs to databases which feed AMS Application for amendments.
- Export files for external systems.

Historical Notes

Prior to the introduction of the Application Management System (AMS), IRIS contained and managed detailed information related to well, road, geophysical and ancillary applications and data associated with their review and determination process. This functionality has since been moved to AMS, but is available through historical READ ONLY versions of the application.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

INTEGRATED RESOURCE INFORMATION SYSTEMS (IRIS)

Classifications of Records that Relate to the System

Schedule Code	Secondary No.	Secondary Title	Retention Schedule A	SA	FD
Data in the System					
OCGO	20200-20	Application files	SO	nil	SR
OCGO	20300-50	Compliance site inspections (covers deficiency reports)	SO	nil	DE
OCGO	20600-30	Facility files	SO	nil	FR
OCGO	20750-45	Incidents	SO	nil	DE
OCGO	20900-20	Road files	SO	nil	FR
OCGO	21000-35	Pipeline projects	SO	nil	FR
OCGO	21700-20	Master licenses to cut	SO	nil	DE
OCGO	21900-30	Well authorization files	SO	nil	FR
OCGO	21900-45	Well incidents – electronic	SO	nil	DE
Inputs					
OCGO	20100-20	Indigenous relations	SO	nil	FR
OCGO	20200-20	Application files	SO	nil	SR
Outputs					
OGCO	20000-10	Statistical and activity reports	SO	nil	DE
Other Related Records					
ARCS	6820-05	Back-up data	SO	nil	DE
ARCS Section 6	see appropriate secondaries	INFORMATION TECHNOLOGY			
102902		Special Schedule for Transitory Electronic Data Processing (EDP) Records	SO	nil	DE

Schedule Code Key: *ARCS = Administrative Records Classification System,* schedule 100001
OCGO = OIL AND GAS REGULATION ORCS, schedule 163507

END OF OVERVIEW

KNOWLEDGE, ENTERPRISE, RESOURCE, MANAGEMENT, INFORMATION, AND TECHNOLOGY (KERMIT)

SYSTEM OVERVIEW

Creating Agency
Oil and Gas Commission

Purpose
KERMIT is a multi-function system that:

- manages the operational lifecycle of pipelines and facilities
- through the corporate registry, includes the interface by which the Commission manages most of the security roles for core Commission systems
- documents operational compliance activities

KERMIT also enables users, both internal and external, to look up legacy applications, find permits, submit notices and submit incidents, and produce reports.

Information Content/Processes

KERMIT is the primary operational management system for pipelines and facilities. It also holds compliance and enforcement information such as inspections, deficiencies, and investigations for all assets (e.g., pipelines, facilities, wells, roads etc.).

KERMIT is also used to:

- Manage name changes, amalgamations, and transfers of assets for activities managed in KERMIT (pipelines and facilities)
- Provide the interface by which internal staff and external company representatives can manage security roles
- Track and manage and liability ratings for wells and facilities (AIR)
- Calculate and report on oil and gas reserves
- Provide general reporting functions, using IRIS data when the reports use well-related data (see the IRIS system overview for IRIS information)

The information in KERMIT is organized by “tabs”, which provide the following functions:

- **To-do List**: part of the workflow element of KERMIT, this information is organized by job type, process type, or user. There are currently over 140 processes that can be performed through this tab, which range from assigning tasks, completing inspections or pipeline cancellations, to entering forest tenure, generating notices, reviewing submitted information, and updating information. The processes tab holds attachments, communication logs and documents and received responses.
- **Post Permit Actions**: this is the area where you can find permits, archaeological requirements, access notices of intent for pipelines and facilities, access legacy applications, update tenure, and start “transactions”, such as notice of construction, notice of pressure tests, as built submissions, etc.
- **Wells:** consisting of legacy data transferred from the decommissioned PIMS system, this contains data such as well index reports, wells spudded, completion data, detailed well inquiries,

year to date well statistics. Well data is actually managed in the IRIS system, but some of it is accessed through KERMIT, primarily through document search and report functions.

- **Projects and Facilities:** this starts with a search page to access pipeline projects and facility information through various criteria such as operations, locations, tenure number, or project number. Once you find your asset (i.e., facility or pipeline project/segment) you have access to multiple tabs outlining information on project/facility details, operational transactions, site equipment, linkages to other data elements such as production or injection data, operator information, design capacity and recovery efficiency, compliance and enforcement actions relating to the site, such as inspections, complaints and incidents, liability information, notes, and attachments.
- **Compliance and Enforcement:** this tab holds emergency management details, i.e,. complaint and incident information; inspections and deficiencies; administrative deficiencies (e.g., when a company isn't submitting required information); and notifications. Notifications of deficiencies, for example, are emailed to the operator through KERMIT, and response is received and logged under the appropriate inspection.
- **Search and maintenance functions:** these tabs cover document search functions, to see what documents have been submitted, and where they reside in the system; also covers system/corporate registry maintenance functions such as entering new contacts, operator changes, bulk cancellations, and is the place to update standardized data elements such as checklists, LMR categories and violation codes.
- **Reports:** KERMIT produces a wide range of reports, categorized into operations, incidents and complaints, community relations, tenure, core, and pipeline reports, some with a range of reports to choose from.
- **Reservoir:** this tab accesses reserves data, produces reservoir reports, disposal well approvals, and a range of reserves and data management reports, which are accessing current data in the IRIS system, as well as data which was transferred to KERMIT from the decommissioned PIMS system. These reports gather information such as pool reserves by oil or gas, engineering pools list, completion events, gas test flow rates, and orphan reserves.
- **Geology:** provides access to geology reports, such as extraneous pools, pay zone contact type issues, pay parameters. These reports are gathering data from IRIS, the system which holds well data.
- **Production:** provides access to production reports, such as monthly and cumulative production, monthly pool production and injection summaries, and also has a production query function, which allows you to search production data through various criteria.
- **Asset Integrity and Retirement:** used to track Liability Management Ratings (LMR), this tab accesses calculators such as well liability calculation detail, facility asset and liability calculation, and runs reports such as operator summary reports, monthly summary reports, and a build report list for wells and facilities.

Historical Notes

Prior to the introduction of the Application Management System (AMS), pipeline and facility applications were submitted to KERMIT. That original application data remains in KERMIT; this includes information

such as application submission documents, First Nation consultation, landowner consultation and notification, communication logs, and the permit.

When the Petroleum Information Management System (PIMS) system was decommissioned, PIMS data was transferred to KERMIT. PIMS was a database of well, facility, reserve, and production related information.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

SYSTEM TITLE (AND ACRONYM)

Classifications of Records that Relate to the System

Schedule Code	Secondary No.	Secondary Title	Retention Schedule A	SA	FD
Data in the System					
OGCO	20000-20	Corporate Registry	SO	nil	DE
OGCO	20200-18	Name changes, transfers and amalgamations	CY+2y	10y	DE
OGCO	20200-20	Application files	SO	nil	SR
OGCO	20300-05	Complaints	SO	nil	DE
OGCO	20300-40	Enforcement case files	CY+14y	nil	DE
OGCO	20300-50	Compliance site inspections	SO	nil	DE
OGCO	20600-30	Facility files	SO	nil	FR
OGCO	20750-45	Incidents	SO	nil	DE
OGCO	20750-50	Major incident and emergency response	SO	nil	FR
OGCO	21000-35	Pipeline projects	SO	nil	FR
Inputs					
OGCO	21900-30	Well authorization files	SO	10y	FR
Outputs					
OGCO	20000-10	Statistical and activity reports	SO	nil	DE
Other Related Records					
ARCS	6820-05	Back-up data	SO	nil	DE
ARCS Section 6	see appropriate secondaries	INFORMATION TECHNOLOGY			
102902		Special Schedule for Transitory Electronic Data Processing (EDP) Records	SO	nil	DE

Schedule Code Key: *ARCS = Administrative Records Classification System,* schedule 100001
OGCO= Oil and Gas Regulation, schedule 163507

END OF OVERVIEW

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
-00	Policy and procedures	Throughout this *ORCS*, all -00 secondaries have been superseded by 21100-00.	Unchanged.
20000 OIL AND GAS REGULATION – GENERAL			
20000-02	Ad-hoc analysis projects	NEW	SO nil DE
20000-03	Energy project review process	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20000-06	Notebooks	NEW	SO nil DE
20000-10	Statistical and activity reports	NEW	SO nil DE
20000-20	Companies	Renamed to Corporate Registry. Supersedes 21000-20. Retention changed from SO 5y DE, and SO trigger defined (added the 5 years into the SO trigger)	SO nil DE

This concordance table is intended as a general guide for transition between the old and new versions of this *ORCS*. The new classifications and retentions apply to all relevant digital and physical operational records, both in the office and in offsite storage. Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

When converting files to the new *ORCS*, you will need to check file contents to ensure that the recommended replacement secondary is appropriate for that particular file.

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20000-25	Geographical Oracle Access Tool (GOAT)	Secondary closed. GOAT was replaced by WHISTLER.	
20000-30	Integrated Resource Information System (IRIS)	Secondary closed as it does not meet *ORCS* standards (we no longer schedule systems with secondaries), and because the 2018 amendment does not include full system analysis which would enable updating it to current standards. Original closing criteria and appraisal note is embedded here for future reference. Original retention was SO nil SR. SO: when the function supported by the database is no longer performed by government SR: The government archives will retain records from IRIS which provide access to the following files: application files - paper (secondary 20200-20), facilities - paper (secondary 20600-30), pipeline projects - paper (secondary 21000-35) and well authorizations - paper (secondary 21900-30). These electronic records serve as an automated index to these files that are fully retained by the government archives. Production, reservoir, engineering and geology related data records may also be retained because they have ongoing scientific and research value. Records in the system related to application status, tracking and sign off have no long-term value and may be destroyed.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
		Decisions about the exact records in the system to be retained and any technical requirements and specifications will be decided in consultation with a government archivist at the time of transfer of records to the government archives.	
20000-40	Compliance evaluation	NEW	SO nil DE
20100 INDIGENOUS RELATIONS			
20100	ABORIGINAL RELATIONS	Primary title changed to INDIGENOUS RELATIONS.	
20100-03	Aboriginal trapping issues	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material. Or, 21600-30 Stakeholder issues.	Unchanged
20100-04	Archaeology	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20100-05	Heritage sites	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20100-06	Traditional use studies	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20100-10	Archaeology impact assessments	Secondary closed. Impact assessments are part of the application file under 20200-20. Retention changed from SO 5y DE.	SO nil SR
20100-12	Archaeology overview assessments	Secondary closed. Overview assessments are part of the application file under 20200-20. Retention changed from SO 5y DE.	SO nil SR
20100-14	Archaeology permit reports	Secondary closed. Use 20250-10 for Final archaeological reports. Retention changed from SO 5y DE.	SO nil DE
20100-16	Site information forms	Secondary closed. Use 20250-10 for Final archaeological reports.	Unchanged
20100-20	Bands / tribal councils	Title changed to Indigenous relations. SO trigger defined. Retention changed from SO 5y SR.	SO nil FR
20100-25	Cross-cultural training	Secondary closed. See -40 Cultural awareness and training. Retention changed from CY+1y 3y DE.	SO nil DE
20100-30	Cultural events	Secondary closed. See -40 Cultural awareness and training.	Unchanged
20100-35	Workshops	Secondary closed. See -40 Cultural awareness and training.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20100-40	Cultural awareness and training	NEW	SO nil DE
20200 APPLICATION REVIEW			
20200-05	Cancelled, expired or refused applications	NEW	SO nil DE
20200-18	Name changes, transfers and amalgamations	NEW (supersedes 21900-18, Well name changes and transfers)	CY+2y 10y DE
20200-20	Application files – paper	Title changed to Application files. SO trigger expanded. Supersedes 20200-25 Application files – electronic.	SO nil SR
20200-25	Application files – electronic	Superseded by 20200-20 Application files. Retention changed from SO nil DE.	SO nil SR
20200-30	General development permits - paper	Title changed to General development permits (GDP). Secondary closed; these permits are no longer issued.	Unchanged
20200-35	General development permits – electronic	Secondary closed; these permits are no longer issued. This classification applies to GDP data held in IRIS.	Unchanged
20200-40	Application review working files	NEW	SO nil DE

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20250 ARCHAEOLOGICAL ACTIVITY MONITORING (NEW PRIMARY)			
20250-05	Borden numbers	NEW	CY+1y nil DE
20250-10	Final archaeological reports	NEW	SO nil DE
20250-20	Declined, cancelled or withdrawn archaeological applications	NEW	SO nil DE
20300 COMPLIANCE AND ENFORCEMENT			
20300-03	Safety	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20300-05	Complaints	NEW	SO nil DE
20300-20	Deficiency reports - paper	Secondary closed. Deficiencies are part of the inspection report on KERMIT, classified under 20300-50.	Unchanged
20300-25	Deficiency reports – electronic	Secondary is closed because these are not tracked in the same way and the data is no longer available.	Unchanged
20300-30	Integrity management – paper	Superseded by 20550-10 Final audit reports, and -20 Audit working files. Retention changed from SO 6y DE.	SO nil DE CY+10y nil DE

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20300-35	Integrity management – electronic	Secondary closed. This information is documented in other parts of the records system.	Unchanged
20300-40	Investigations	Title changed to Enforcement case files. Retention changed from SO 6y DE.	CY+14y nil DE
20300-45	Compliance issue and topic files	NEW	SO nil DE
20300-50	Site inspections - paper	Title changed to Compliance site inspections. Supersedes 20300-55 Site inspections – electronic. Retention changed from SO 6y DE, and SO trigger updated.	SO nil DE
20300-55	Site inspections – electronic	Superseded by 20300-50 Compliance site inspections.	Unchanged
20300-60	Contravention decisions	NEW	SO+10y nil FR
20300-65	Orders	NEW	SO+10y nil FR
20400 DISPUTE RESOLUTION – CLOSED PRIMARY			
This primary is closed. The Commission stopped using the Alternative Dispute Resolution (ADR) framework in 2010 when the Oil and Gas Activities Act came into effect, and dispute facilitation was no longer regulated. Because these records are scheduled for full retention, the information from the primary is here to assist in the transfer of the records to the government archives.			

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
Records relating to the commission's role in resolving oil and gas development issues and disputes between affected parties, such as energy companies and landowners or First Nations. The goal of dispute resolution is to explore and understand each other's interests and develop acceptable solutions together. If the commission cannot resolve the dispute, it must encourage the use of consensual alternative dispute resolution. Pursuant to the *Oil and Gas Commission Act* (SBC 1998, c. 39, s. 8), the commission may authorize one or more persons to facilitate settlement, and make recommendations that must be considered by the commission before deciding the disputed matter. Pursuant to the *Oil and Gas Commission Act* (SBC 1998, c. 39, s. 9), the advisory committee's role in requests for reconsideration is that upon application by an interested person, the advisory committee may request that the commission reconsider any original decision made. The Commission may grant or refuse the request and reconsider the matter in a manner the commission deems appropriate. This primary also covers the practice advisory group (PAG), a joint initiative between the commission and the oil and gas industry. The PAG structure consists of a steering committee and eight sub-committees that submit recommendations to the commission.			
20400-20	Alternative dispute resolution (ADR) Secondary is closed	(arrange by name of individual or company) (covers background documentation, decisions, recommendations and related ADR correspondence involving companies or individuals) FR: The government archives will fully retain alternative dispute resolution (ADR) records because these records provide evidence of citizens' concerns about the oil and gas development process and the commission's central role in resolving outstanding issues and disputes between parties.	CY+1y 9y FR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20400-25	Oil and gas commission advisory committee Secondary is closed	(covers minutes, reports, briefing notes, recommendations and decisions) FR: The government archives will fully retain oil and gas advisory committee records because these records provide evidence of the deliberations and advice of citizens, representing environmental, First Nations, and other interests, to the Oil and Gas Commission.	CY+1y 9y FR
20400-30	Practice advisory group (PAG) Secondary is closed	(covers issues, concerns, suggestions and recommendations submitted to PAG and subsequent issue papers developed for submission to the commission) FR: The government archives will fully retain practice advisory group (PAG) records because these records provide evidence of the deliberations and advice of citizens, representing scientific, oil and gas industry, and government interests, to the Oil and Gas Commission.	CY+1y 9y FR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20400-40	Requests for reconsideration Secondary is closed	(covers background documentation, recommendations and related correspondence from the advisory committee concerning requests for reconsideration) FR: The government archives will fully retain requests for reconsideration because these requests provide evidence of citizen involvement in the resolution of issues and disputes related to the oil and gas development. These records are also related to the oil and gas advisory committee records (secondary 20400-25) that are retained by the government archives.	CY+1y 9y FR
20500 ENGINEERING AND GEOLOGICAL MONITORING – PRIMARY CLOSED			
20500-02	Enhanced oil (tertiary) recovery	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-04	Environmental	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-05	Experimental scheme	Superseded by 21400-35 Reservoir analysis and management Retention changed from CY+2y 2y DE.	SO nil FR
20500-07	Infill drilling	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20500-08	Flaring	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-09	Gas conservation	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-10	Gas cycling	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-13	Gas re-injection	Superseded by 21400-35 Reservoir analysis and management. Retention changed from CY+2y 2y DE.	SO nil FR
20500-14	Injection / disposal	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-15	Surface casing reductions	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20500-18	Waivers	Superseded by 21400-35 Reservoir analysis and management or, by the well file the waiver applies to. Retention changed from CY+2y 2y DE.	SO nil FR
20500-20	Monthly injection / disposal statements (BC S-18 forms)	Secondary closed – original retention applied to paper based processes, and these forms are received through e-submission and go into IRIS. Create a new schedule for the data when doing the full system overview of IRIS, and system transformation has stabilized.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20550 EXTERNAL AUDIT AND COMPLIANCE ASSESSMENT (NEW PRIMARY)			
20550-10	Final audit reports	NEW	SO nil DE
20550-20	Audit working files	NEW	CY+10y nil DE
20600 FACILITIES REGULATION AND MONITORING			
20600-03	Facilities index	Secondary is closed – indexes are no longer created. Original SR: The government archives will selectively retain the facility index because it provides access to facilities - paper (secondary 20600-30) records that are retained by the government archives. Commission staff will transfer a copy of the current (at the time of transfer) facility index with each accession of facilities - paper files. If the facility index is discontinued, the last version of the index will be fully retained. All other versions may be destroyed because the list is cumulative and the information will be captured in the versions that are fully retained.	Original retention (unchanged): SO nil SR
20600-20	Emergency response plans - production	Secondary superseded by 20750-20 Emergency response plans (ERP's).	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20600-30	Facilities – paper	Name changed to Facility files. Supersedes -35 Facilities – electronic. Closing trigger redefined, and retention changed from SO+1y 10y FR.	SO nil FR
20600-35	Facilities – electronic	Superseded by 20600-30 Facility files. Retention changed from SO nil DE.	SO nil FR
20600-40	Facility incidents – paper	Secondary superseded by 20750-45 (incidents are not separated by the type of activity they relate to). Retention changed from SO+2y 10y DE.	SO nil DE
20600-45	Facility incidents – electronic	Superseded by secondary 20750-45.	Unchanged
20700 GEOPHYSICAL EXPLORATION – PRIMARY CLOSED			
20700-02	Flow holes	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20700-03	Trappers	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20700-04	Unexploded charges	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20700-20	Geophysical (seismic) program files – paper	Secondary is closed; these are now Investigative Use Permits (IUP) under 20200-20. The retention still applies to records offsite: SO+3y 10y DE. SO trigger: when the final plans are received.	Unchanged
20700-25	Geophysical (seismic) program files - electronic	Secondary is closed; these are no longer being created. Data still resides in IRIS.	Unchanged
20750 INCIDENT AND EMERGENCY RESPONSE – NEW PRIMARY			
20750-05	Company correspondence	NEW	CY+9y nil DE
20750-07	Emergency Management BC reports	NEW	CY+1y nil DE
20750-20	Emergency response plans (ERP's)	NEW Supersedes: • 20600-20 Emergency response plans – production (facilities). Retention: SO nil DE • 21000-25 Emergency response plans (pipeline) Retention: SO nil DE • 21900-20 Emergency response plans - drilling and completion Retention: SO+1y nil DE (SO = when production emergency response plan is submitted)	SO nil DE

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20750-30	Exercise evaluations	NEW	SO nil DE
20750-45	Incidents	NEW Supersedes: • 20600-40 Facility incidents - paper Retention: SO+2y 10y DE • 20600-45 Facility incidents – electronic Retention: SO nil DE • 21000-45 Pipeline incidents – paper Retention: SO+2y 10y DE • 21000-50 Pipeline incidents – electronic Retention: SO nil DE • 21500-30 Rig incidents Retention: SO+2y 10y DE • 21900-40 Well incidents - paper Retention: SO+2y 10y DE • 21900-45 Well incidents – electronic Retention: SO nil DE SO for paper files: when the incident is resolved. SO for electronic files was undefined.	SO nil DE
20750-50	Major incident and emergency response files	NEW	SO+10y nil FR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20800 LAND USE PLANNING – PRIMARY CLOSED			
20800-03	Agricultural impact assessments	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-04	Agricultural land commission	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-05	Environmental impact assessments	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-07	Habitat conservation	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-08	Issues	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-10	Protected areas	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-12	Stream crossings	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
20800-20	Land resources management planning (LRMP)	Superseded by 20000-02 Ad-hoc analysis projects. Retention changed from CY+1y 2y DE.	SO nil DE

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20800-30	Muskwa-Kechika management area	Superseded by 20000-25 Ad-hoc analysis projects. Retention changed from CY+1y 2y DE.	SO nil DE
20850 LIABILITY MANAGEMENT – NEW PRIMARY			
20850-03	Security deposit files	NEW. Supersedes 21900-03.	SO+1y 9y DE
20850-20	Corporate asset files for orphaned or at risk sites	NEW	SO nil DE
20850-21	Corporate asset files for transferred assets	NEW	SO nil OD
20900 ROAD REGULATION AND MONITORING			
20900	PETROLEUM DEVELOPMENT ROAD (PDR) APPROVAL	Primary title change to ROAD REGULATION AND MONITORING. This reflects the fact that PDR's are no longer issued, they are now simply "road permits", and permit approvals are scheduled under 20200.	
20900-07	Sierra Yoyo Desan (SYD) road	Secondary closed. NOTE: This classification would cover topical material. Commission records related to issuing this road permit, and subsequent material, should be on the PDR Road file, under 20900-20. The retention for 20900-20 is SO+5y nil FR.	Unchanged.

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
20900-20	Petroleum development roads (PDR) – paper	Secondary renamed to Road files. Scope changed: original PDR files contained both the application and activity, whereas new road files contain the activity information, and the permit approval is classified under 20200-20. SO trigger defined. (supersedes 20900-35)	Unchanged
20900-25	Petroleum development roads (PDR) - electronic	Secondary is closed because these are no longer being issued. Retention is SO nil DE. Did not merge this classification with the paper because the data had been appraised as DE, and the nature of the data hadn't changed to warrant re-appraisal (the "official" PDR file was maintained in paper format).	
20900-30	Road use permits – paper	Superseded by 20200-20 Application files. Retention changed from SO+1y nil DE.	SO nil SR
20900-35	Road use permits – electronic	Superseded by 20200-20 Application files. Retention changed from SO nil DE.	SO nil SR
21000 PIPELINE REGULATION AND MONITORING			
21000-03	Bridge crossings	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091 -

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21000-05	Pipeline codes and standards	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21000-06	Pipeline index	Secondary is closed - indexes are no longer created. Original SR criteria: The government archives will selectively retain the pipeline index because it provides access to pipeline projects - paper (secondary 21000-35) records that are retained by the government archives. Commission staff will transfer a copy of the current (at the time of transfer) pipeline index with each accession of pipeline projects - paper files. If the pipeline index is discontinued, the last version of the index will be fully retained. All other versions may be destroyed because the list is cumulative and the information will be captured in the versions that are fully retained.	Original retention (unchanged): SO nil SR
21000-07	Pipeline information bulletins	Secondary is superseded by 21600-06 External communications. Retention changed from CY+1y 2y DE.	CY+3y 6y FR
21000-09	Tank farms	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21000-20	Companies	Secondary is closed (it can still be applied to offsite records). Company files are now classified under 20000-20 Corporate Registry. Retention changed from SO 5y DE.	SO nil DE
21000-25	Emergency response plans	Secondary superseded by 20750-20 Emergency response plans (ERP's).	Unchanged
21000-30	Environmental assessment projects	Secondary closed. Function transferred to Major Projects, which will be covered in future ORCS amendment.	
21000-35	Pipeline projects - paper	Name changed to Pipeline projects. Supersedes -40 Pipeline projects – electronic.	SO nil FR
21000-40	Pipeline projects – electronic	Superseded by -35 Pipeline projects. Retention changed from SO nil DE.	SO nil FR
21000-45	Pipeline incidents – paper	Secondary superseded by 20750-45 (incidents are not separated by the type of activity they relate to). \Retention changed from SO+2y 10y DE.	SO nil DE
21000-50	Pipeline incidents – electronic	Superseded by secondary 20750-45.	Unchanged.
21000-55	Pipeline Information System (PLS)	Secondary is closed. The data in PLS was migrated to KERMIT when the system was decommissioned.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
		21100 POLICY AND PROCEDURE DEVELOPMENT	
21100-00	Policy and procedures	Scope expanded to cover all policy and procedures for the Commission. Simplifies scheduling when many products span multiple primaries.	Unchanged.
21100-02	Checklists	Closed, as there is no evidence of use. Newly created lists may be scheduled under 100-05.	Unchanged.
21100-20	Guideline and policy development files	Added SO trigger. Retention changed from SO+2y 5y DE.	SO 5y DE
21100-25	Levies and fees	Secondary closed. Levies and fees, per *OGAA*, are now established in regulation; files relating to amendments to levies and fees are scheduled under *ARCS* primary 140.	Unchanged.
		21200 PRODUCTION MONITORING – PRIMARY IS CLOSED	
21200-02	Crown petroleum natural gas rights	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material. for new / onsite material. . (Ministry of Energy, Mines and Petroleum Resources is responsible for this function)	Unchanged.
21200-03	Drilling activity	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21200-04	Gas production and reserves	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-06	Numerical simulation	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-07	Oil and gas activity	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-08	Oil production and reserves	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-10	Periodic progress reports	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-11	Revenue	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21200-13	Statistics	Superseded by 20000-10 Statistical and activity reports.	Unchanged.
21200-15	Studies and analysis	Closed because secondary is unused. Ad hoc analysis projects are classified under 20000-02. Studies and research will be properly covered in future ORCS amendment.	Unchanged.
21200-20	Petroleum Information Management System (PIMS)	Secondary is closed. Data was migrated to Kermit when the system was decommissioned.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21200-30	Production audits	Secondary is closed – no longer doing these.	Unchanged.
21300 PROJECT FUNDING – PRIMARY CLOSED			
		Primary is closed because the original funding program, SCEK, was superseded by the BC Oil and Gas Research and Innovation Society (BC OGRIS), which acts as an independent society. The commission no longer receives the project applications, as outlined in the original schedule. Commission staff who are on a BC OGRIS committee or board will schedule their records under *ARCS* primary 200.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21300-20	Environmental fund projects - pending/approved	Secondary is closed. Original SO: when project is complete Original SR criteria: The government archives will selectively retain environmental fund project records. Only a copy of each final project report will be fully retained. The research documented in these reports has ongoing scientific value. These reports also provide detailed information about the type of projects funded by the commission and its industry partners. All remaining records, including applications for funds and administration of funds, may be destroyed. A summary list of approved projects and amounts awarded is available in the commission's annual report (secondary 21600-20) that is fully retained by the government archives. At the time of transfer to off-site storage commission staff will box final reports separately from other records that will be destroyed.	Original retention (unchanged): SO+1y 6y SR
21300-30	Environmental fund projects - rejected/discontinued	Secondary is closed. Original retention: CY+1y 4y DE.	Unchanged
21300-40	Other funded projects	Secondary is closed. Original retention: CY+1y 2y DE.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
		21400 RESERVOIR REGULATION AND MONITORING	
21400-02	Acid gas	Covers acid gas progress reports. Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-03	Annual pressure survey schedule	Superseded by 21900-20 Well authorization files. Retention changed from SO NA NA.	SO nil FR
21400-04	Concurrent production	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-06	Gas cap production	Superseded by 21900-20 Well authorization files. Retention changed from SO NA NA.	SO nil FR
21400-08	Good engineering practice	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-09	Hydrocarbon and by-products reserves report	Superseded by 21600-20 Annual activity reports. Retention changed from SO NA NA.	SO nil FR
21400-10	Pool drainage	Superseded by *ARCS* 358-20 Library/topical reference material. Retention changed from SO NA NA.	SO nil DE
21400-11	Storage of hydrocarbons in underground formations	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21400-13	Waterflood	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-20	Commingling	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-30	Field designations	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-35	Reservoir analysis and management files	NEW	SO nil FR
21400-40	Natural gas allowable production	Title changed to Production allowable reports. Retention changed from SO NA NA.	SO 7y DE
21400-50	Pool designations and lists	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21400-60	Reservoirs	Superseded by -35 Reservoir analysis and management. Retention changed from SO NA NA.	SO nil FR
21500 RIG REGULATION AND MONITORING – PRIMARY CLOSED			
21500-03	Rig activity	Secondary is superseded by 21900-30 Well authorizations. Rig activity information is received through e-submission and filed to the well file.	SO nil FR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21500-05	Rig lists	Secondary is closed – weekly rig activity lists are no longer being produced. Original retention was CY+1y 2y DE.	
21500-20	Rigs	Secondary is closed – rig information is being maintained on the well file, under 21900-30.	SO nil FR
21500-30	Rig incidents	Secondary superseded by 20750-45 (incidents are not separated by the type of activity they relate to). Retention changed from SO+2y 10y DE.	SO nil DE
		21600 STAKEHOLDER RELATIONS	
		Primary title changed from STAKEHOLDER COMMUNICATION.	
21600-02	Commissioner's update	Secondary closed – now part of the Pipeline newsletter, under *ARCS* primary 312.	
21600-05	Information bulletins	Superseded by 21600-06 External communications. Retention changed from CY+1y 2y DE.	CY+3y 6y FR
21600-06	Information letters	Title change to External communications. Supersedes 21600-05 Information bulletins. Retention changed from CY+1y 2y DE.	CY+3y 6y FR
21600-10	Preliminary mediation	Secondary closed – not a process that is used anymore.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21600-12	Public involvement guideline	Secondary closed – not being produced anymore.	
21600-20	OGC annual reports and service plans	Title changed to Annual activity reports. SO trigger defined.	
21600-25	Pre-application issues case files	SO trigger defined.	SO nil DE
21600-30	Report development files	NEW	SO nil DE
21600-35	Stakeholder issues	NEW	SO nil DE
21600-40	Strategic engagement projects	NEW	SO+7y nil DE
21700 TIMBER CUTTING LICENSING			
		Primary title changed from TIMBER CUTTING LICENCE MONITORING.	
21700-02	Forest Practices code	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material	Unchanged
21700-03	Master License Index	Secondary is closed – no longer maintaining this index.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21700-20	Master licenses to cut – paper	Title changed to Master licenses to cut. Retention changed from SO+2y 3y DE to reflect current practice.	SO nil DE
21700-25	Master licenses to cut – electronic	Secondary closed – not used in IRIS, as indicated. If Master License to Cut data is created, it will be scheduled under -20.	
21800 WASTE REGULATION – PRIMARY CLOSED			
21800-02	Contaminated sites	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-03	Deep well disposal	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-04	Drilling spills	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-05	Drilling waste	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material	Unchanged
21800-07	Emissions	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material	Unchanged
21800-09	Land spraying while drilling	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21800-10	Operator registration lists	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-12	Sour liquids	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-13	Special waste	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-14	Storage of waste	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-16	Waste discharge	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-17	Water disposal	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21800-20	Waste management permits	Secondary superseded by 20200-20 Application files. This secondary was established before the Commission began issuing waste management permits. Retention changed from SO+1y 5y DE	SO nil SR

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-091

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
		21900 WELL REGULATION AND MONITORING	
21900-02	Coalbed Methane (CBM)	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21900-03	Drilling deposits	Superseded by 20850-03. Retention changed from FY+1y 5y DE	SO+1y 5y DE
21900-04	Drilling reports	Superseded by 21900-30, because drilling reports are part of the well file. Monthly drilling reports exported from IRIS are covered by 20000-10.	SO nil FR
21900-05	Drilling techniques and technology	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21900-08	Field pressures	Superseded by 21900-30. Field Pressures are filed onto the appropriate well files. Retention changed from CY+2y 3y DE.	SO nil FR
21900-09	Offshore drilling	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21900-13	Segregation tests	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21900-14	Sour gas	Closed. Use ARCS 358-20 Library/topical reference material for new / onsite material.	Unchanged
21900-15	Spacing and target areas	Superseded by 21400-35 Reservoir analysis and management Retention changed from CY+4y nil DE	SO nil FR
21900-17	Well index	Secondary is closed - indexes are no longer created. SR: The government archives will selectively retain the well index because it provides access to well authorizations - paper (secondary 21900-30) records that are retained by the government archives. Commission staff will transfer a copy of the current (at the time of transfer) well index with each accession of well authorizations - paper files. If the well index is discontinued, the last version of the index will be fully retained. All other versions may be destroyed because the list is cumulative and the information will be captured in the versions that are fully retained.	Original retention (unchanged): SO nil SR
21900-18	Well name changes and transfers	Superseded by 20200-18 Name changes, transfers and amalgamations.	CY+2y 10y DE
21900-20	Emergency response plans – drilling and completion	Secondary superseded by 20750-20 Emergency response plans (ERP's). Retention changed from SO+1y nil DE.	SO nil DE

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
21900-30	Well authorizations – paper	Title changed to Well authorization files. Supersedes -04 Drilling Reports, -08 Field Pressures, -35 Well authorizations – electronic, and 21500-05 Rig activity. SO trigger redefined. Retention changed from SO+1y 10y FR.	SO nil FR
21900-35	Well authorizations – electronic	Superseded by -30 Well authorizations. Retention changed from SO nil DE.	SO nil FR
21900-40	Well incidents – paper	Secondary superseded by 20750-45 (incidents are not separated by the type of activity they relate to). Retention changed from SO+2y 10y DE.	SO nil DE
21900-45	Well incidents – electronic	Superseded by secondary 20750-45.	Unchanged
SYSTEM OVERVIEW SECTION			
	Application Management System (AMS)	NEW	
	Geographical Oracle Access Tool (GOAT)	System overview closed; GOAT has been replaced by Whistler, which will be covered in a future ORCS amendment.	
	Integrated Resource Information System (IRIS)	AMENDED	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

Request BCER2024-001

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

APPENDIX A: Summary of Amendments to the *OIL AND GAS REGULATION ORCS*

Primary/ Secondary	Title	Type of Change	New retention A/SA/FD
	KERMIT	NEW	
	Petroleum Information Management System (PIMS)	System overview closed; PIMS has been decommissioned.	
	Pipeline Information System (PLS)	System overview closed; PLS has been decommissioned.	
	Oil and Gas Commission Website	Overview closed as it is no longer applicable. The Commission website is undergoing a complete overhaul at the time of ORCS amendment, and will be appraised in a future amendment.	

Any records in offsite storage that are classified by a secondary that is now closed may finish their lifecycle with the original retention.

Key to *ARCS/ORCS* Codes and Acronyms

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
20000	**OIL AND GAS REGULATION - GENERAL**		
25000-01	General *(throughout the ORCS)*	CY+1y nil DE	Keep for two years, and then destroy.
20000-02	Ad-hoc analysis projects	SO nil DE	When the project relates to a plan or policy, keep until it has been abandoned or approved, and there is no need to refer to the records; and for all other ad hoc analysis projects, keep until they no longer have reference value, and then destroy.
20000-06	Notebooks	SO nil DE	Keep until you do not refer to them, and then destroy.
20000-07	Oil and Gas Commission website	SO nil DE	Webpages will be deleted as they are updated, redesigned or closed.
20000-10	Statistical and activity reports *(ad hoc, statistical and routine reports (i.e. weekly/monthly/quarterly) that are not part of an operational file, such as a compliance file or well file)*	SO nil DE	Keep until no longer required for statistical, reporting or analysis purposes, and then destroy.
20000-20	Corporate Registry	SO nil DE	Keep until it has been five years since the company ceased operations in the province, or, for longstanding companies, when 12 years have elapsed from the receipt of the information. Then destroy.
20000-40	OGC Board of Directors files	FY+1y 8y FR	Keep for ten years, and then transfer to the government archives.
20000-40	Compliance evaluation files *(for the compliance work done outside of the C&E team, or in conjunction with them)*	SO nil DE	Keep until any outstanding issues have been resolved, and when no longer useful for researching a company's compliance history, and then destroy.
20100	**INDIGENOUS RELATIONS**		
20100-20	Indigenous relations	SO nil FR	Keep until no longer required to support the Commissions' relationship and document the history with Indigenous communities, and then transfer to the government archives.

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
20100-40	Cultural awareness and training	SO nil DE	Keep until no longer used or referenced, and then destroy.
20200	**APPLICATION REVIEW**		
20200-05	Cancelled, expired, or refused applications	SO nil DE	Keep until four years has elapsed and no activity has occurred since application approval, or since refusal of the application, and then destroy.
20200-18	Name changes, transfers and amalgamations	CY+2y 10y DE	Keep for 12 years, and then destroy.
20200-20	Applications *(Covers all permits and licence applications received and approved by the Commission)*	SO nil SR	Keep until all permits and licences have expired, conditions have been met, and, where relevant, the retentions in the associated activity files have expired. Keep archaeological permits until no longer required to provide evidence of permitted archaeological activities. Then most applications will be transferred to the government archives. *(see ORCS for details)*
20200-40	Application review working files *(Covers the working files of anyone in the Commission who is part of the application review process.)*	SO nil DE	Keep until you are no longer referring to them, usually after application is approved and activity has commenced, and then destroy.
20250	**ARCHAEOLOGICAL ACTIVITY MONITORING**		
20250-05	Borden numbers	Cy+1y nil DE	Keep for two calendar years, and then destroy.
20250-10	Final archaeological reports	SO nil DE	Keep until no longer useful for reference purposes, and then destroy.
20250-20	Declined, cancelled or withdrawn archaeological permits	SO nil DE	Keep until no longer required for reference when reviewing subsequent archaeological applications, and then destroy.
20300	**COMPLIANCE AND ENFORCEMENT**		
20300-05	Complaints	SO nil DE	Keep until complaint is closed and is no longer required for statistical reporting or trend analysis, and then destroy.

Key to *ARCS/ORCS* Codes and Acronyms

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
20300-40	Enforcement case files	CY+14y nil DE	Keep for 15 years, and then destroy.
20300-45	Compliance issue and topic files	SO nil DE	Keep until reference value has expired, and then destroy.
20300-50	Compliance site inspections	SO nil DE	Keep for inspections associated with a permitted activity, when the retention period for the activity (such as a well authorization) has expired; for general inspections not associated with a permitted, when 10 years have elapsed since remediation actions were completed, and then destroy.
20300-60	Contravention decisions	SO+10y nil FR	Keep for 10 years after administrative penalties have been paid and review and appeal periods have expired, and then transfer to the government archives.
20300-65	Orders	SO+10y nil FR	Keep for 10 years after conditions of the order have been satisfied and review and appeal periods have expired, and then transfer to the government archives.
20550	**EXTERNAL AUDIT AND COMPLIANCE ASSESSMENT**		
20500-10	Final reports	SO nil DE	Keep until no longer required for tracking a company's history of compliance with their regulatory requirements, and then destroy.
20500-20	Audit working files	CY+10y nil DE	Keep for 10 years after the audit year is complete, and then destroy.
20600	**FACILITIES REGULATION AND MONITORING**		
20300-30	Facility files	SO nil FR	Keep until the facility has been removed, the site has been restored, and the file is no longer required to document activities conducted on the site. Then transfer to the government archives.
20750	**INCIDENT AND EMERGENCY RESPONSE**		
20750-05	Company correspondence	CY+9y nil DE	Keep for 10 years, and then destroy.
20750-07	Emergency Management BC reports	CY+1y nil DE	Keep for 2 years, and then destroy.
20750-20	Emergency response plans (ERP's)	SO nil DE	Keep until there have been three subsequent plans received, or when the asset that the supplemental plan relates to has had a certificate of restoration issued or remedial actions completed.
20750-30	Exercise evaluations	SO nil DE	Keep until no longer required to monitor whether a company is meeting response objectives and commitments; this will usually be two full exercise cycles (6 years), and then destroy.

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
20750-45	Incident files	SO nil DE	Keep until the incident is complete, and the information is no longer relevant for site reclamation, and then destroy.
20750-50	Major incident and emergency response files *(covers the records of the EOC)*	SO nil FR	Keep until the incident is complete, and the information is no longer relevant for site reclamation, and then transfer to the government archives.
20850	**LIABILITY MANAGEMENT**		
20850-03	Security deposit files	SO+1y 9y DE	Keep for 10 years after the security has either been returned to the company, transferred to another operator, or transferred to the Orphan Site Reclamation Fund, and then destroy.
20850-20	Corporate asset files for orphaned or at risk sites	SO nil DE	Keep until no longer useful to support the transfer of the site or the reclamation of the orphaned site, and then destroy.
20850-21	Corporate asset files for transferred assets	SO nil OD	Keep until the ownership of the asset has been transferred to the responsible party / new permit holder, and then transfer the file/s to them.
20900	**ROAD REGULATION AND MONITORING**		
20900-20	Road files	SO+5y nil FR	Keep for 5 years after the road has been cancelled or deactivated, and restoration is complete, and then transfer to the government archives.
21000	**PIPELINE REGULATION AND MONITORING**		
21000-35	Pipeline projects	SO nil FR	Keep until the pipeline has been removed, or no longer exists, and then transfer to the government archives.
21100	**POLICY AND PROCEDURE DEVELOPMENT**		
25100-00	Policy and procedures – final *(covers both internal and external policies, guides, manuals, best practices, etc.)*	SO 5y FR	Keep 5 years after the policy is replaced or becomes irrelevant; for policy/procedures which are required to provide point-in-time evidence, such as environmental and wildlife policy, when no longer needed to provide evidence for decisions, then transfer to the government archives.
25100-20	Policy, guideline, and procedure development files	SO 5y DE	Keep for 5 years after the final product is approved and distributed, or abandoned and when no longer referred to, and then destroy.
21400	**RESERVOIR REGULATION AND MONITORING**		
21400-25	Geological topical files	SO nil DE	Keep until no longer useful for reference purposes, and then destroy.

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
21400-35	Reservoir analysis and management	SO nil FR	Keep: • records relating to production management, such as GEP's, until it has been 20 years since pool abandonment; • records relating to projects that resulted in a changed subsurface environment or have potential safety considerations in future activities, such as disposals and waterflood projects, until no longer required to provide evidence of the activities; • records which document the composition and structure of the field or pools, until that information is no longer required. Then transfer to the government archives.
21400-40	Production allowable reports	SO 7y DE	Keep for 7 years after the end of the production year, and then destroy.
21600	**STAKEHOLDER RELATIONS**		
21600-06	External communications	CY+3y 6y FR	Keep for 10 years, and then transfer to the government archives.
21600-20	Annual activity reports *(this covers all Commission reports produced on an annual basis)*	SO nil FR	Keep until no longer when being used for trend analysis and understanding Commission and activity history, and then transfer to the government archives.
21600-25	Pre-application issues case files *(this applies to landowner liaison case files and includes archaeology as well)*	SO nil DE	Keep until the issue is resolved or no longer relevant, or the permit is approved and activity has commenced, and when no longer needed for reference and tracking purposes. Then destroy.
21600-30	Stakeholder issues *(covers the resolution of issues and concerns that are not related to specific permits, applications, or part of the pre-application process)*	SO nil DE	Keep until issue is resolved or no longer topical, and when no longer needed for reference purposes, and then destroy.
21600-35	Strategic engagement projects	SO+7y nil DE	Keep for seven years after the project is completed, cancelled, or abandoned, and then destroy.

APPENDIX B: SUMMARY OF RETENTIONS – *please refer to the ORCS document for classification details.*

Classification	Classification Title	Retention	Retention (in narrative form)
21600-40	Report development files *(this covers the development / draft material for producing the annual reports under -20.)*	SO nil DE	Keep until report has been published, or abandoned, and when development material is no longer required for reference purposes, and then destroy.
21700	**TIMBER CUTTING LICENSING**		
21700-20	Master licences to cut	SO nil DE	Keep until replacement master license is issued, and then destroy.
21900	**WELL REGULATION AND MONITORING**		
21900-30	Well authorization files *(there is a clarifying note in the ORCS describing why this will be an indefinite period)*	SO nil FR	Keep until a certificate of restoration is issued, and the well information is no longer needed for environmental and safety management, then transfer to the government archives.

BC Oil & Gas COMMISSION

M365

INFORMATION MANAGEMENT IN ONEDRIVE

Microsoft OneDrive

Microsoft (MS) OneDrive is a cloud based personal workspace provided to each Microsoft 365 user for information and materials related to their work. Records within OneDrive can only be accessed by the user, unless they specifically grant permission to share a document with another person(s).

As OneDrive implementation evolves, guidance will be updated.

Recordkeeping roles and responsibilities

To comply with the *Information Management Act*, the Commission must retain all official records in an appropriate recordkeeping system.

OneDrive is not an appropriate repository for long-term storage of Commission records: information is not accessible to others who may need it (e.g. when an employee is absent); and information is not easily searchable for FOI or legal requests. Keeping information in OneDrive creates information silos.

It is intended for short-term storage of records being actively worked on, i.e. drafting a new document, or personal reference material.

Employees are responsible for ensuring critical information that they create or receive is filed in an appropriate recordkeeping system (most often, within folders on our shared drives).

Critical Records include official or final copies, substantial drafts, correspondence, and other records that document decisions and actions.

Documenting Commission Decisions

If records in OneDrive contain important decisions, or context for those decisions, they must be retained. For more information on the requirements to document decisions, see the Documenting Commission Decisions resource material.

Freedom of Information and Protection of Privacy roles and responsibilities

Information in OneDrive is subject to requests under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Freedom of Information (FOI): Employees are responsible for information searches in response to FOIPPA requests and other legal obligations within their OneDrive.

Protection of Privacy/Confidentiality: Although it is a personal workspace, OneDrive supports collaboration through the ability to share OneDrive documents through Teams or emails. When sharing a document, care must be taken to ensure sensitive or confidential material is only viewed by those who need to see it.

Limit sharing sensitive or confidential information (e.g. personal information), as you would with any communication tool; for example, when sharing a link in an email, check that only the appropriate people have access.

BC Oil & Gas COMMISSION

WHAT MUST I DO WITH INFORMATION IN ONEDRIVE?

Each employee is responsible to ensure information is appropriately managed in the OneDrive environment.

File critical information on OneDrive to a recordkeeping system, i.e. shared drives.

Because OneDrive is not an appropriate recordkeeping system, and critical information is to be filed elsewhere, OneDrive should only hold transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information may be deleted when no longer needed.

One Drive is similar to your F: drive as your individual storage space. This is a place to store information and documents that you are not ready to make official or share with your team yet, or that are for your personal use only. You are the only person with access to your OneDrive.

You can store personal copies of HR-type records, convenience copies of reference material, and drafts – until they are finalized, or ready to share with your team.

Share documents carefully.

You are responsible for managing permissions to documents you store in your OneDrive. When you select permissions, you are choosing who will be able to access your document. Only give permission to individuals who need to access the information. There are a few ways to share documents in OneDrive; be sure to select the sharing method which is appropriate to the sensitivity of the document.

Best practice

Regularly review your OneDrive and routinely transfer any official records to your recordkeeping system. Delete any transitory information that is no longer needed.

Consult the Official vs Transitory Records guide to learn more about what you should move to a shared drive, and what you can delete.

BC Oil & Gas COMMISSION

MANAGING INFORMATION IN SHAREPOINT

Microsoft SharePoint

SharePoint is a document management and collaboration tool in Microsoft Office 365. It is used to collaborate and share content across an organization. It can also be used as a records management tool. This guide provides advice and guidance on using SharePoint to manage commission records.

Under *the Information Management Act* (IMA), government bodies must ensure that an appropriate system is in place for creating and maintaining government information. If managed appropriately, SharePoint can be part of that system.

Planning to implement SharePoint

Implementing a SharePoint site should involve the same careful planning as required for any system implementation. This generally includes the following steps:

A. Requirements gathering and analysis
B. Gaining and maintaining management commitment and support for the project
C. Pre-implementation architecture, design, configuration and testing
D. Establishing governance, user training, and communications protocols
E. Post-implementation testing and monitoring
F. Post-project document migration to a recordkeeping system and closing the SharePoint site

Assign responsibility for managing and filing records at the start. Do not wait until the site project/purpose is over before identifying who needs to manage and file the documents into the appropriate recordkeeping system.

SharePoint Site Owners are responsible for:

- Identifying appropriate site users and permissions.
- Creating and managing document Libraries and Content Types.
- Ensuring documents are migrated to a recordkeeping system at project completion or site closure.

This guide only applies to the M365 SharePoint application.

It does not apply to records and information in Teams.

Teams uses SharePoint for short-term collaboration. However, Teams is not an approved recordkeeping system under the IMA. Once you are finished collaborating on a document in Teams, it should be saved to your recordkeeping system.

Do not keep final document versions in Teams SharePoint for long-term storage

BC Oil & Gas COMMISSION

Site Owners are responsible to ensure information is appropriately managed in the SharePoint environment.

Using SharePoint to manage your records

There are many ways to use and configure SharePoint. The following best practices provide some basic records management measures for the records maintained there:

- **Establish and document responsibility for the site and access to it. Keep that documentation up to date.** Site Owners need to ensure all access permissions are kept current. This enables authorized staff to locate the records and information they need for operational, FOI or other legal purposes.
- **Implement an ARCS and ORCS structure upfront.** SharePoint sites should be organized according to approved information schedules (ARCS/ORCS). This involves mapping site content to specific record classifications. Contact Records and Information Services for guidance on how to do this.
- **Document design and configuration decisions.**
- **Use naming conventions for documents.** Try to consistently title documents with established naming conventions, or using standard elements (e.g. a clear description of the document, version number, and creation date).
- **Delete transitory information regularly.** Information management rules apply to records in SharePoint. Transitory records may be routinely deleted by employees. All other records must follow the retention schedules outlined in ARCS/ORCS.

FOI, Privacy and Confidentiality of Information

Information in SharePoint is subject to access requests under the *Freedom of Information and Protection of Privacy Act* (FOIPPA). When using SharePoint, ensure you:

- Are prepared to respond with copies of responsive records for FOI or other legal obligations.
- Limit sharing personal, sensitive or confidential information to only what is necessary for conducting Commission business.

Shutting down your SharePoint site?

Contact Records and Information Services first.

Your records may need to be migrated to a recordkeeping system once the site is no longer in use.
We will help guide you on the best course of action.

BC Oil & Gas COMMISSION

M365

MANAGING INFORMATION IN TEAMS

Microsoft Teams

Microsoft (MS) Teams is a communication and collaboration tool in Office 365. Features include one-on-one chats, team chats, document collaboration, video meetings, and integration with other shared applications. Each MS Team has a designated Team Owner.

Page one in this guide identifies our legislated requirements and responsibilities in the Teams environment. Page two clarifies how we manage our information in Teams.

Recordkeeping Roles and Responsibilities in Teams

The Commission is governed by legislation and policy which requires us to create and keep adequate records of our decision-making and work activities.

Teams does not have the necessary functionality and controls for an appropriate recordkeeping system. It is a tool for communication and collaboration. When working in Teams:

Employees need to ensure critical information that they create in Teams is filed in an appropriate recordkeeping system (most often, this is our shared drives).

Team Owners are ultimately responsible for ensuring critical information within their Teams sites is filed in the recordkeeping system.

Critical information includes official or final copies, substantive drafts, correspondence, and other records that document decisions and actions.

You may have critical information in meeting recordings, chat messages, collaborative documents, or Planner tasks.

When documenting decisions made in Teams, remember to include the context for that decision (e.g. the discussion or chat thread that lead to the decision). For more information, see the Documenting Commission Decisions resource material.

Freedom of Information and Protection of Privacy (FOIPPA) Roles and Responsibilities in Teams

Freedom of Information (FOI):
As with all Commission records, information in Teams may be requested under FOIPPA. When working in Teams:

Team Owners, under the direction and guidance of the FOI team, are responsible for ensuring records searches are done in response to FOI requests and other legal obligations.

Employees should be prepared to respond to a records search request when notified by a Team Owner.

Protection of Privacy/Confidentiality:

Employees should try to limit sharing personal, confidential or sensitive information, as you would with any communication tool. When sharing information in Teams, remember that Team membership may change over time and include external employees or contractors.

BC Oil & Gas COMMISSION

WHAT MUST I DO WITH INFORMATION IN TEAMS?

Team Owners are responsible to ensure information is appropriately managed in the Teams environment.

File critical information from MS Teams to a recordkeeping system:

Because Teams is not an appropriate recordkeeping system, Teams primarily holds transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information is eligible for deletion when no longer needed.

Everything you do in Teams should be for collaboration purposes only. This is not a place to store documents for future use or preservation purposes. Once you are finished collaborating on a document, it should be saved to your recordkeeping system (shared drive).

Final versions of documents should not be kept in Teams for long term storage.

Manage chat messages:

Avoid using Team chats for conversation that will have operational/strategic value and must then be managed. If this happens, you must document these chat messages in a retainable format, such as a memo or email which can be stored on a shared drive:

- Copy, summarize, or transcribe the information to another document, and
- File it in your recordkeeping system.

Understand chat retentions

It is important to understand how long your chat messages remain in Teams, so that you can save critical messages in time:

- Ad hoc chat messages outside Teams channels will be deleted in 10 days.
- Department/branch Teams chat messages will be deleted from Teams after 3 months.
- Project or committee Teams chat messages remain in Teams for the duration of the project.

Save critical records from external Teams:

If you are part of a Team for an inter-jurisdictional committee, the host Team's retention rules govern the information shared in the Team space. Ensure critical records for the Commission's role in the committee are captured in the recordkeeping system.

Best Practice

Regularly review your Teams documents and chat channels, and copy out any information that is critical to your operations, or part of an official record.

Consult the Official vs Transitory Records guide to learn more about what you should move to a shared drive, and what you can leave in Teams as transitory information.

ISSUANCE: **People, Reconciliation and Transformation Division**
Information Systems & Technology

APPROVED: June 14, 2023

1.0 GENERAL

1.1 Purpose

This policy is intended to guide employees in the suitable use of BC Energy Regulator (BCER) information and technology (IT) resources. Employees are required to sign off annually on the policy.

This policy has been developed to:

- Promote IT knowledge and appropriate resource usage throughout the organization.
- Maximize productivity and minimize risks to BCER network security and performance.
- Protect the privacy, confidentiality, and security of BCER information systems, technology, and information (e.g., data, documents, records, content, etc.).
- Improve adherence to government information and technology-related legislation, policies, and standards.
- Promote public trust in the BCER's use of information and technology assets.

Any questions regarding the interpretation or application of this policy should be directed to the Executive Director, Information Systems & Technology, or to the Director, Information Technology.

1.2 References

- *Employee Code of Conduct and Ethics Policy*
- *Information Security Policy*
- *BC Office of the Chief Information Officer Security Policy*
- *Government Core Policy and Procedure Manual* section 12.3
- *Freedom of Information and Protection of Privacy Act*
- *Mobile Device Policy*
- *Managing Confidential Information Guide*
- *Building Access and Security Policy*
- *Information Management Act*
- *Information Management Policy*
- *Interim Privacy Breach Notification Policy*

1.3 Application and Scope

Employees shall use IT resources in accordance with the Employee Code of Conduct and Ethics policy. As a condition of employment, employees are expected to take responsibility for, and accept the duty to, actively protect BCER information and technology assets. This includes being aware of, and adhering to, all relevant legislation, policies, and standards.

Improper use may jeopardize the confidentiality, integrity, and availability of BCER information and technology assets, and put personal and/or sensitive information, security, and service levels at risk.

2.0 POLICY

2.1 IT resources refers to BCER owned hardware and software, including but not limited to:

- Laptops, desktops, tablets
- Mobile phones
- Web conferencing
- BCER email
- Monitors, mice, keyboards, headsets
- Docking stations
- Data projectors, USB sticks

2.2 The purchase of hardware, software, and cloud services will be done through the Information Systems and Technology department and may require:

- The completion of a fair procurement process; and/or
- A completed privacy impact assessment (PIA) and security threat and risk assessment (STRA).

2.3 Regarding the use of IT resources, employees have an obligation to not:

- Circumvent or subvert the BCER Information Security Policy, cybersecurity controls or procedures.
- Leave BCER devices unattended and unlocked whether in the office or while working remotely.
- Use non-BCER approved services (e.g., AI language models, private cloud storage, email, file transfer, etc.) or devices to send, receive or exchange information about the BCER.
- Save BCER information on local hard drives of workstations, laptops, tablets, or mobile phones except as defined in Section 2.8.
- Use IT resources in a manner that inappropriately discloses, shares or compromises BCER information.
- Use natural language AI models with inputs with specific BCER information. Inputs must be genericized.
- Use IT resources in a manner that violates Canadian or BC laws.
- Use IT resources in a manner that negatively impacts or disrupts BCER business or operations.
- Use IT resources to download non-work-related files (e.g., Freeware, Shareware, illegally obtained movies or music files); Stream video over BCER network resources, unless the access is work-related and authorized.
- Install unauthorized applications on BCER devices.
- Share BCER login credentials with others.
- Record password(s) in a manner that could compromise security (e.g., on sticky notes left on monitors, inside desk drawers or under pen/pencil trays, etc.).

2.4 Any content created, received, or transmitted using BCER equipment or retained within the BCER's network will be appropriately managed as a BCER record in accordance with applicable legislation and policy.

2.5 There can be no expectation of personal privacy related to the use of BCER information technology resources except for specific privileged communications (i.e., Cabinet,

solicitor/client, and union representative communications).

2.6 Any collection, access, use and/or disclosure of Personal Information must be done in accordance with the *Freedom of Information and Protection of Privacy Act* and its supporting policies. This includes mandatory completion of a PIA to assess and mitigate risks.

2.7 If an information/privacy breach (i.e., unauthorized file access) or cybersecurity incident occurs, employees and supervisors must report to the BCER's Cybersecurity team and designated Privacy Officer(s) without delay.

2.8 Only while employees are traveling or working remotely may work related documents be saved on a local hard drive temporarily. Priority when working remotely is to use GlobalProtect to access BCER files or systems. Local hard drive files should be deleted once in the office.

2.9 Employees must be cybersecurity aware. This includes completing mandatory training and practices such as using strong passwords, scrutinising email for phishing attacks and reporting suspicious links or files.

3.0 LIMITED PERSONAL USE

3.1 Employees are permitted limited personal use of BCER IT resources. Personal use of BCER IT resources should not occur during peak hours (i.e., 8 a.m. to 5 p.m. weekdays) and must be consistent with the Employee Code of Conduct and Ethics and Information Security policies.

3.2 Personal use of BCER pooled IT resources (during or outside of office hours) must be approved by the resource owner and scheduled through the Resource Scheduler.

3.3 Storage of personal pictures, music, or videos on an employee's local workstation (C: drive), tablet or mobile phone is acceptable; however, they must not be stored on the network. IT does not back up these types of files.

4.0 APPROVAL

Approved by the Executive Team on June 14, 2023

Version Control:

Revision V1	Dec-13	Administrative Updates
Annual Review	Oct-14	No Changes
Annual Review	Oct-15	No Changes
Revision V2	Nov-16	Added Sections 2.3 - 2.5
Revision V3	Dec-17	Administrative Updates
Annual Review V4	Nov-18	No Changes
Annual Review V4	Apr-20	Administrative Updates (Title)
Revision V5	23-Jun	Updated Policy

BRITISH COLUMBIA **ENERGY REGULATOR**

POLICY

Policy Name	Use of IT Resources Policy
Policy Number	UP1
Approving Authority	Executive
Designated Executive Officer	Sara Dickinson, Executive Vice President, People, Reconciliation & Transformation
Effective Date	August 06, 2024
Last Reviewed	June, 2024
Next Review	April, 2025

1.0 PURPOSE

The purpose of this policy is to ensure that BCER's Information Technology (IT) resources, provided to employees to enhance their productivity, are used responsibly and ethically, and in compliance with BC Government legislation and BCER policies. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing any system of their obligation to exercise good judgment.

Any questions regarding the interpretation or application of this policy should be directed to one of the following:

- Executive Director, Information Systems & Technology.
- Director, Information Technology.
- Director, Information Security.

2.0 APPLICATION AND SCOPE

This policy applies to all IT Resources that are managed by the BCER, including computers, software, communication devices, network, and cloud-based devices and software.

Employees shall use IT Resources in accordance with the Employee Code of Conduct and Ethics policy. Employees are required to take responsibility for and actively protect BCER information and technology assets. This includes being aware of, and adhering to, all relevant legislation, policies, and standards.

Improper use may jeopardize the confidentiality, integrity, and availability of BCER information and technology assets, and put personal and/or sensitive information, security, and service levels at risk.

3.0 DEFINITIONS

A. **IT Resources**: Refers to the technology, information/data assets provided by the organization to its employees to enhance their productivity, including but not limited to:
   - Laptops, desktops, tablets.
   - IT peripherals such as monitors, mice, keyboards, headsets, docking stations.
   - Corporate Property issued mobile phones.
   - Storage media such as USB sticks, hard drives.
   - Data (such as BCER email, network files).
   - Software and cloud services such as M365 (Teams, Word, Excel, PowerPoint, One Drive).
   - Other devices with a network connection or requiring software.

B. **Large Language Models**: A type of artificial intelligence algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate, and predict new content.

4.0 POLICY REQUIREMENTS

A. Employees must not access and/or purchase technology, devices, applications, or services (known as “shadow IT”) that are not authorized and approved by Information Systems & Technology (IST). Purchases must include a fair procurement process and the completion of a Privacy Impact Assessment (PIA) and Security Threat and Risk Assessment (STRA).

B. The use of Artificial Intelligence (AI), including Large Language Models, within the BCER must follow principles of ethical conduct, transparency, and accountability.

C. IT Resources and BCER issued accounts must be used only by the employee to whom they have been assigned.

D. Employees must always protect all corporate-managed IT Resources, ensuring they are physically and logically secured and remain under the employee's control. IT Resources must not be left unattended and/or unlocked, whether in the office or while working remotely.

E. All content created, received, transmitted, or retained for BCER business purposes must be appropriately managed as a BCER record in accordance with applicable legislation and policy.

F. BCER documents and information must only be stored within BCER managed systems. Work-related documents may only be copied to a local hard drive while employees are offline, however, they must be copied back to BCER managed systems as soon as the employee returns from the remote location.

G. BCER employees have limited personal privacy when using business resources. Business resources may be subject to collection of information for freedom of information requests, security investigations, or other purposes.

H. The collection, access, use and/or disclosure of Personal Information must be done in accordance with the Freedom of Information and Protection of Privacy Act. Any new or revised collection, access, use and/or disclosure of Personal Information must first be approved via the BCER Privacy Impact Assessment process to ensure identification, assessment, and mitigation of risks.

I. Information/privacy breaches (e.g. unauthorized file access) or cybersecurity incidents must be reported to the BCER's Cybersecurity team and designated Privacy Officer(s) without delay.

J. A strong cybersecurity posture is the collective responsibility of all BCER employees. Active participation in cybersecurity training sessions and adherence to best practices (such as creating and maintaining strong passwords, exercising vigilance in identifying and reporting phishing attempts, and promptly reporting any suspicious activity) is mandatory. Employees must not circumvent or subvert the BCER Information Security Policy, cybersecurity controls or procedures.

K. Good IT Resource hygiene must be practiced. This includes following IST instructions, notifications, and device maintenance prompts to ensure systems are secure, reliable, and up to date with features and functionality.

L. Employees are permitted limited personal use of BCER IT Resources if personal use of BCER IT Resources does not impact business operations and is consistent with the Employee Code of Conduct and Ethics, Information Security Policy, Canadian law, and British Columbia laws.

5.0 RELATED LEGISLATIVE REFERENCES

- Freedom of Information and Protection of Privacy Act
- Information Management Act

6.0 RELATED BCER POLICIES

- Employee Code of Conduct and Ethics Policy
- Information Security Policy
- Mobile Device Policy
- Managing Confidential Information Guide
- Building Access and Security Policy
- Information Management Policy
- Procurement policy

7.0 AUTHORITIES AND OFFICERS

a) Approving Authority – Executive
b) Designated Executive Officer – Sara Dickinson, Executive Vice President, People, Reconciliation & Transformation
c) Procedural Authority – Executive
d) Procedural Officer – Ab Dosil, Executive Director, Information Systems & Technology

INFORMATION LOCATIONS IN THE COMMISSION							
Record type	Record locations			Contact	Program area	FOI notes	Notes
	electronic	paper	system				
Land use planning review	K: drive / outlook			Sean Curry	Operational Policy & Environment		
Corporate Registry / company files			KERMIT	Shannon Weatherill / Jody	Permitting		FSJ base for this function
Name changes / amalgamations /	K: drive	offsite	TANC	Shannon Weatherill / Jody	Permitting		
Board of Director records	K: drive / outlook	offsite		Stacey Bligh	Board Services		
Archaeology				Vera Brandzin	Heritage Conservation		
Archeaology permits	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Archeaology non-compliance files	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Archaeology audits	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Indigenous relations - strategic	K: drive	offsite		Kelly Wintemute	Strategic Engagement		Prince George base for
Indigenous consultation - applications	K: drive	Application file in FSJ File Room (pre-2016)	AMS since 2016	Adam Kamp / Ryan Stark	Permit Adjutication / Decision Support		FSJ base for this function
Indigenous agreements	K: drive	?		Kelly Wintemute	Strategic Engagement		
Indigenous awareness and training	K: drive			Kelly Wintemute	Strategic Engagement		
Applications (for activity permits)		Application file in FSJ File Room (pre-2016)	AMS since 2016	Shannon Weatherill / Jody Sutherland	Permitting		Including well, geothermal (since 2018), pipeline, facility, LNG facility, road, geophysical permits and all associated oil and gas
Applications for EMA activities		EMA files in FSJ file room		Rachel Butler	Operational Policy & Environment		
Applications for ARCH acitivities		ARCH files in FSJ file room		Vera Brandzin	Heritage Conservation		
Geothermal wells	K: drive	Kelowna offices (?)	"IRIS mirror system"	Jordan ven Besouw	Drilling Engineering & Technical Services		
Application review - Indigenous consultation working files				Adam Kamp / Ryan Stark	Permit Adjutication / Decision Support		
Application review - LNG projects	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	FTP site, AMS for final notes (since	Suzanne Matthews	Drilling Engineering & Technical Services		
Application review - Archaeological	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	AMS for final notes (since 2016)	Vera Brandzin	Heritage Conservation Program		

Application review - Engineering	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	AMS for final notes (since 2016)	Kevin Parsonage	Engineering, Integrity & Technical Compliance		
Application review - Geological	K: drive		AMS for final notes	Jeff Johnson	Petroleum Geology		
Complaints			KERMIT		C&E		
Enforcement invesitgation cases	K: drive				C&E		
Inspections - compliance	K: drive (still?)		KERMIT		C&E		
Contravention decisions	K: drive			Andy Johnson	C&E		
Orders: compliance	K: drive			Andy Johnson	C&E		
Orders: s. 75	K: drive			Ron Stefik	Reservoir Engineering		Reservoir engineering
Orders: securities (s. 30)	K: drive			Wade Abbott / Mike Janzen	Liability Management		Orphan and Liability
Orders: s. 38							
Integrity Management Program - external audit	K: drive	Kelowna offices		Gouri Bhuyan	Engineering, Integrity & Technical Compliance		Covers IMPS (pipelines?), FIMPS (facilities) & DIMPS
Restoration Verification Audit program	K: drive	FSJ File Room		Akbar Ali Khan	Operational Policy & Environment		Audits of well site reclamation.
Facilities		FSJ File Room	KERMIT	?	Kelowna		
Incidents	K: drive	FSJ File Room	KERMIT	Peter Dalton	Security and Emergency Management		Incidents are tracked in KERMIT, major incidents
ERP (Emergency Response Plans) program	K: drive			Peter Dalton	Security and Emergency Management		
Emergency Response Plans			ERP Database	Peter Dalton	Security and Emergency Management		
Emergency Response Exercises	K: drive			Peter Dalton	Security and Emergency Management		
Security deposits - Liability	K: drive			Wade Abbott / Mike Janzen	Liability Management		
Roads - applications		Application file in FSJ File Room (pre-2016)	AMS (since 2016)	Jody Sutherland	Permitting		
Roads - activity files		FSJ File Room		Jody Sutherland	Permitting		
Pipeline projects - applications		Application file in FSJ File Room (pre-2016)	AMS (since 2016)				
Pipeline projects - activity files		FSJ File Room					
Policies - corporate	K: drive			Julie Barker	Corporate Properties & Administration		
Procedures - according to program							

Geological studies	K: drive	Offsite		Jeff Johnson	Petroleum Geology		
Field and Pool / Reservoir Management	K: drive	Offsite		Ron Stefik	Reservoir Engineering		Covers water disposal, good engineering practice (GEP), concurrent production, waterflood, gas reinjection, experimental/innovative
Production allowable reports	K: drive	Offsite		Ron Stefik	Reservoir Engineering		
External Communication products	K: drive			Graham Currie	Public & Corporate Relations		Covers information letters, industry bulletins,
Annual Reports	K: drive			Graham Currie?	Public & Corporate		
Landowner Liaison	K: drive	Dawson Creek office		Laura-Lea Gibson / Laurie Phillips	Community Relations (Applications)		
Strategic engagement	K: drive			Kelly Wintemute (Indigenous), Corey Jonsson (stakeholder)	Public & Corporate Relations		
Master licences to cut		FSJ File Room		Jody Sutherland	Permitting		
Well files - technical		Offsite	IRIS / E-library	Rob Story	RIS		
Well files - field files / post		FSJ File Room	IRIS / E-library	Terri Marsh	RIS		
Area Based Analysis			ABA	Krista Zens	GIS, Operational Policy & Environment		
Eeyore mapping data			EEYORE	Jody Sutherland	Permitting		
Geospatial data				Krista Zens	GIS, Operational Policy & Environment		
Process Mapping			Process Central	Rob Mitchell	Process Improvement, Analysis & Planning		
Delegation of Authority	K: drive			Lauren Krakau (legal)	Legal Services		
Legal records / cases / etc.	K: drive	Offsite		Sara Gregory	Legal Services		
Major Projects					Major Projects,		

EXTRA INFORMATION:

Refer to this document for detailed information: Media notes by ORCS classification:

file:///K:\RIM%20Victoria\ORCS%20Development%20432-40\OGCO%20ORCS%20Amendment%201\Project%20admin%20and%20background\Media%20notes%20by%20classification.docx

EDRMS Needs Assessment

For the BC Oil & Gas Commission

Version 2

April 30, 2021

STATEMENT OF CONFIDENTIALITY

This document is the property of NTT DATA and is produced in response to your request. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, to parties outside your organization without prior written permission from NTT DATA. For more details, see Legal Notice © 2021 NTT DATA, Inc.

REVISION HISTORY

Version	Effective Date (DD/MM/YYYY)	Brief Description of Change	Affected Section(s)	Prepared By	Reviewed By	Approved By

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

TABLE OF CONTENTS

1 Executive Summary 4
1.1 Key Findings 4
1.2 Key Risks 4
2 Overview 6
2.1 Background 6
3 Methodology 7
3.1 Compliance Rating System 8
3.2 Project Tasks 9
4 Findings and Recommendations 11
4.1 Records Management Governance 11
4.2 Records Classification and Retention Schedule 16
4.3 Electronic Records Management 20
4.4 Information Protection 24
4.5 Information Flow and Retrieval 27
5 EDRM System Business Requirements 30
6 EDRM Road Map 31
7 Conclusion 32
8 Acknowledgements 33

Appendix A – Questionnaire Results – Summarized

Appendix B – EDRM System Business Requirements

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

1 Executive Summary

In February 2021, the BC Oil and Gas Commission (the Commission) engaged NTT DATA to perform an assessment of business requirements for an Electronic Document and Records Management (EDRM) system to support the management of the Commission's unstructured electronic records, and further the development and enhancement of an EDRM Program and related services.

To prepare this report, NTT DATA conducted a series of data gathering activities. A survey was submitted and workshops conducted with representatives from Records and Information Services (RIS) and Information Technology (IT). The following report is a summary of findings and recommendations as well as EDRM business requirements that comprise the main deliverables of the project.

Based on the Five foundational components of records management, the questionnaire results indicated the following overall maturity level of the Commission's Records Management program:

RM COMPONENTS	MATURITY LEVEL
• RM Governance	• Level 3 (essential)
• Records Classification & Retention	• Level 3 (essential)
• Electronic Records Management	• Level 1 (sub-standard)
• Information Protection	• Level 5 (transformational)
• Information Flow & Retrieval	• Level 2 (essential)

.

1.1 Key Findings

Much work has already been planned, initiated and, in many cases, completed by the RIS Branch to advance and implement records management best practices and critical foundational work necessary for supporting an EDRM system. For example, the branch has: hired specialist FTEs, modernized the Operational Records Classification System (ORCS) Records Schedule to achieve media neutrality, reflect current standards and the Commission's business environment; engaged an external Records and Information Management (RIM) consultant to classify and schedule unstructured official records stored on shared drives; and developed a wide range of corporate policies, guidelines and educational resources.

It has been evident for some time that the Commission requires appropriate electronic document management tools and additional resources to support the organization in the midst of a rapidly evolving digital business environment. Participants stressed that the current electronic information environment demands controls consistent with EDRM system functionality in order to meet strategic and operational business goals, legislative and policy compliance requirements, and address growing risks associated with information inaccessibility, loss and preservation. The need for an EDRM system has been identified in RIS branch strategic planning documentation (e.g. Information Governance RIM Strategy and Tactical Plan) and included as a project in the Commission's current Corporate Initiatives Register.

1.2 Key Risks

A fully implemented EDRM system can protect an organization from significant risks such as data loss, compliance issues, public relations crises, confidentiality breaches, security threats and disaster recovery. A well-executed system helps to mitigate these risks in much the same way that an insurance policy does – by acting as a safeguard against unexpected future events. A comprehensive EDRM system outlined in the recommendations can help to reduce the Commission's exposure to risk in the following areas:

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

- Decision Making Risk - Not having information available when and where necessary can lead to incorrect decision-making based on incomplete, out-of-date or inaccurate information. Making the wrong decision due to inadequate supporting documentation leads to and may compound the risk exposure in other areas such as financial risk, safety risk and increased costs.
- Financial Risk - Fines can be incurred, money misspent, lawsuits lost, audits unfavorable or opportunities missed when information collections are out of date or incomplete.
- Litigation & Audit Risk – There are a multitude of scenarios involving information management and litigation or audits. Having the appropriate documentation to prove or disprove a claim is one of the key elements to a favorable outcome of an audit or legal action.
- Legislative Compliance Risk – The inability to locate and produce requested records under the Freedom of Information and Protection of Privacy Act (FOIPPA) can lead to formalized complaints, subsequent investigations and potential penalization by the Office of the Information and Privacy Commission. Similarly, non-compliance with the Information Management Act (IMA) can lead to government oversight and intervention. Media reports about legislative non-compliance can contribute towards reputational risk and loss of public trust which would be especially harmful to a regulatory public body.
- Efficiency and Operating Cost Risk – Organizational efficiency can be seriously impaired if needed information is not readily available. Costs for additional staff, office space and records storage can skyrocket when records and document controls are not followed. Also, in the event of litigation or complex audits, internal costs to manage the abundance of 'documentary evidence' can be minimized with a well-organized records program.
- Emergency Preparedness Risk - Allowing documents to go unfiled and unmanaged for extended periods of time creates a risk of losing track of vital records in the event of a disaster.

Designed to minimize risk and maximize efficiency and compliance, this report contains detailed recommendations and requirements to improve and manage the unstructured electronic records environment with emphasis on the configuration of an EDRM system for the Commission. These recommendations are practical and reasonable requirements that must be supported by an implementation plan that addresses change management and user support at all stages.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

2 Overview

2.1 Background

The Oil and Gas Commission (Commission) is the provincial single-window regulatory agency responsible for regulating oil, gas and renewable geothermal activities in British Columbia, including exploration, development, pipeline transportation and reclamation. Core responsibilities include reviewing and assessing applications for proposed industry activities, consulting with First Nations, co-operating with partner agencies, and ensuring industry complies with provincial legislation and all regulatory requirements.

The Commission has been rapidly transitioning to become a fully digital organization; however, digital records management has not kept pace. As a result, the Commission finds itself without a system to effectively manage the end-to-end life cycle of its unstructured electronic records (records outside of established information systems).

In addition, the province's legislative framework (Information Management Act) has evolved to modernize and streamline government information management by transitioning to digital storage and information management practices.

Microsoft 365

The Commission is currently migrating to Microsoft Office 365 (M365) and Azure for enterprise usage. M365 combines a suite of online services, including email, cloud file storage, and secure communication tools along with the traditional desktop applications. A subsequent gap analysis project was anticipated in order to evaluate the commission's records management and user requirements against the functionality M365 offers.

Senior Management understands that well managed information is a valuable and irreplaceable information asset and that in the midst of a rapidly evolving digital business environment, it is essential that records be managed effectively and proactively. For that reason, in February 2021, the Commission engaged NTT DATA to develop "A records management requirements document establishing specific criteria for the Commission, which will serve as the framework for a gap analysis against functionality implemented with Microsoft 365".

The deliverables of this project are the following report of findings, recommendations and EDRM business requirements. Through a balanced combination of objective, quantifiable data and more descriptive, qualitative observations, the report provides the Commission with the essential information it needs to identify gaps and provides a clear benchmark of the functionality required for managing their digital information assets.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

3 Methodology

This project followed a carefully designed methodology for assessing, developing, and implementing any records management (RM) program. In this case, the methodology has been applied to an EDRM Program. The methodology has been built according to five foundational components of records management. The Foundational Components of Records Management comprise a common-sense approach based on the key principles expressed in the International Standard ISO 15489: Information and documentation: Records management.

ISO 15489 is a two-part policy and procedural framework that businesses need to follow to ensure that they create, retain and manage records adequately. Compliance with this standard also facilitates compliance with other ISO standards, such as the broadly recognized ISO 9000 and ISO 14000.

ISO standards reflect the combined work of more than 100 national standards bodies from around the world, facilitating a more efficient exchange of goods and services across borders and legal systems.

By reflecting these universally recognized standards, NTT DATA's methodology ensures not just direct compliance with the ISO standards themselves, but also that electronic records are retained, protected and made available in a way that supports compliance with any applicable laws, regulations and generally accepted practices.

The Five Foundational Components of RM are as follows:

The bulk of this report is organized according to the Five Foundational Components. Each section of the report will explain the Component in more detail, as well as its practical implications for the Commission. Following the details of the Five Components is the EDRM Business Requirements.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

3.1 Compliance Rating System

For each interview, the Project Team used a rating system to assign a Compliance Score within the Five Foundational Components. These Component scores were then used to complete an overall score for the Commission. NTT DATA developed this rating system to allow for a more objective and consistent assessment of compliance levels. While it is not intended to reflect badly on any particular area, it does allow an organization to see where it is doing well and highlights those areas which will need further enhancements in order to reach a higher level of records management compliance.

The Project Team asked specific questions within each Component to measure how close the Commission is to achieving ideal compliance with the ISO standard. Each answer was given two separate scores. First, an answer was given an objective score based on simple 'yes/no' criteria. Then, the answer was scored more subjectively based on the perceived effectiveness of any practices or documentation linked to that yes/no answer. A summary of questions and responses can be found in Appendix A – Questionnaire Results Summarized.

Scoring Table

Score (Yes/No)	Subjective Score	Subjective rationale
Yes (2)	Compliant (2)	Documented processes to meet all key legal requirements and industry standards; Clear, reasonably easy to implement; and Applied to all applicable records
Yes/No (1)	Sometimes/ Informal/Partial compliance (1)	Documented processes but some gaps re: compliance; or No documented processes, but informal practices widely observed.
No (0)	Not Compliant (0)	No documented processes or informal practices; Documented processes but serious inadequacies threaten legislative compliance and/or practical implementation; or Documented processes generally not applied or implemented
n/a (--)	n/a (--)	Given requirement not applicable.

For example, NTT DATA asked representatives whether records are retained long enough to meet legal requirements. The respondents indicated that the Records Schedules are up to date. Although these Schedules are in place, it has not been applied to electronic content. This answer was given a top mark of 2 in the yes/no column, because there are existing Records Schedules, but only a 1 in the subjective column because retentions have not been applied to electronic records. All answers were totaled, and an overall score given for each of the five foundational components.

Are you reasonably confident that records are retained long enough to meet legal requirements and offer defence against litigation risks?	Yes	2		Risk that records have been kept longer due to retentions not being applied to electronic records.	1	
		Qualitative Score			Subjective Score	

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

Maturity Model

While the foundational components identify the critical hallmarks of information management, the Maturity Model defines characteristics of various levels of recordkeeping programs. The five levels of the Model are as follows:

Records Management Program Maturity Model

Level 1 (sub-standard) 1 – 20 %
- Record keeping concerns not addressed at all or in a very ad hoc manner
- Organization should be concerned that programs will not meet legal or regulatory scrutiny

Level 2 (in development) 21 - 40 %
- Developing recognition that recordkeeping has an impact on the organization
- Organization may benefit from a more defined information governance program
- Organization still vulnerable since practices ill-defined and still largely ad-hoc

Level 3 (essential) 41 – 60 %
- Minimum requirements addressed
- Defined policies and procedures
- Specific decisions taken to improve recordkeeping
- May still be missing significant opportunities for streamlining business and controlling costs

Level 4 (proactive) 61 – 80%
- Initiating information governance improvements
- Information governance routinely integrated into business decisions
- Easily meets legal and regulatory requirements
- Consider business benefits of global information availability

Level 5 (transformational) 81 – 100 %
- Routine integration of information governance into infrastructure and business processes
- Recognized effective information governance critical in cost containment, competitive advantage and client service

Although an overall rating can be assigned, most organizations will be at differing levels of maturity depending on the characteristic being evaluated.

3.2 Project Tasks

Start-up Meeting

A start up meeting was held on February 18, 2021. Participants included Kathryn Smerechinskiy, Rob Smith, Mahia Frost and Dana Keough for the Commission and Joan Sparkes and Claire Connelly for NTT DATA. The meeting provided NTT DATA and the Commission an opportunity to discuss project details and ensure consensus with respect to the planned scope, methodology and tasks.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

Gap Analysis: Structured Data Gathering and Workshops

The main goal of the project was to understand the current electronic and physical records environment and identify existing gaps and areas of records and information management which would be translated into EDRM requirements. The basis of this assessment was a questionnaire completed by the IS and RIS groups and workshops with the same individuals.

EDRMS Business Requirements

The EDRMS Business Requirements were developed using the Ministry of Management Services Request for Proposal - Enterprise Document and Records Management System as the key point of reference. Although issued in 2001, many of the requirements identified in the Request for Proposal are still functionally relevant today. The Business Requirements were reviewed within a workshop setting and summarized within this report.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4 Findings and Recommendations

4.1 Records Management Governance

An appropriate corporate governance structure is essential to any records management program which complies with applicable laws, regulations and industry standards. ISO 15489 outlines the key components of a records management governance structure:

- A corporate policy endorsed at the highest level of the executive and defining the authorities, responsibilities, roles and interrelationships of all personnel who manage or perform records management processes;
- A corporate policy statement that provides auditing of compliance with the organization's records management program;
- Designation of one or more individuals at the management-level who will promote, monitor and enforce compliance with the records management program on behalf of the entire organization;
- Clear and direct statement of practices which should be avoided or performed only with special permission from a designated authority;
- Outlining of records management responsibilities in all applicable job descriptions or equivalent documents; and
- An appropriate form and level of training for all designated records management personnel and any personnel with significant responsibility for records creation and/or control.

4.1.1 Findings – Records Management Governance

Overall compliance levels within this Component were as follows:

RM Governance	**59% - Level 3 (essential)**

Legislative authority for overall records management compliance in the province is provided through the Information Management Act (IMA), an element of which requires the management of government records through information schedules, such as the Administrative Records Classification System (ARCS), Operational Records Classification System (ORCS) and other applicable schedules (e.g., Executive Schedule, Transitory Records Schedule).

As a key governance initiative, ORCS was re-developed as required under the IMA legislation and deemed essential for the appropriate management of Commission records. Approved for use in 2019, ORCS forms the operational framework and modernizes the original ORCS to current standards and

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

positions the Commission to become EDRM ready. Phase 1 of ORCS development was designed to apply classifications and retentions to most Commission program records saved on the network. Those records remaining will be addressed in ORCS Phase 2.

ORCS Phase 2 development is required under the IMA legislation and for the appropriate management of Commission data and records within systems. Phase 2 entails a detailed analysis of all Commission systems holding operational data and records. As well, the RIS Branch will examine the suitability of ARCS Schedules for administrative, financial, and human resources related information. ORCS Phase 2 has been initiated and is a long-term initiative.

Responsibilities for records management officially come under the jurisdiction of the Director Records and Information Services (RIS) Branch and six full time staff members. There are no dedicated administrative positions outside of this branch. There are individuals that manage their records as part of their overall duties although there is no formal delegation of responsibilities for records outside of RIS.

There are a range of guidelines and policies available on the Commission intranet and a Confidential Information Management Guide forms part of the annual sign-off process with the Code of Conduct for each employee. Additional materials are currently under development (e.g. Digitization Policy, Email Management Guide).

The entire Commission organization was trained in elements of the IMA through Documenting Commission Decisions workshops. The ORCS development process familiarized some areas with information schedules. Program specific RM training has been provided on an as-needed basis as well as training and information sessions on Freedom of Information and Protection of Privacy Act (FOIPPA) requirements.

4.1.2 Recommendations – Records Management Governance

NTT DATA recommendations for the Commission under the Component of Records Management Governance are divided into four areas:

4.1.2.1 EDRM Roles and Responsibilities

To support an EDRM Program, consider establishing a dedicated EDRM Business Analyst, on either a full time or contract basis. In collaboration with IS, the role of the business analyst is to support the planning, introduction and roll out of the new EDRM system. Within context of EDRM functionality, the Business Analyst would be responsible for the following:

- Examine existing business processes and identify critical records collections,
- Identify gaps in processes and opportunities for improvements and automation,
- Capture requirements, create site mockups,
- Generate technical requirements, proof of concept solutions,
- Help implement the new processes, features, and tools, and

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

- Document improvements, measure progress, repeat the process, and
- Deliver training to users on system functionality.

Directly address day-to-day Department Site Administration records management responsibilities (e.g. maintaining electronic file directories, granting permissions to Team Sites) as part of the position responsibilities for administrative support personnel, where appropriate.

4.1.2.2 EDRM Procedures and Best Practices

The Commission will be required to develop EDRM procedures to direct the program. The focus will be on the development of detailed department specific work procedures and practices on such topics as:

- Document repository overview – 'where to store' rules i.e. EDRM/OneDrive/etc
- Navigating the EDRM System and Department Sites
- EDRM Roles and Expectations
- Classifying and Naming Department Specific Electronic File Collections
- Adding and revising documents within EDRM
- Sharing documents from EDRM
- Searching the EDRM repository

4.1.2.3 EDRM Training and Awareness

Concurrent with the completion of EDRM procedure and practices, it is recommended that the Commission develop a EDRM Training and Awareness Plan to proactively ensure compliance with its program. Appropriate training and awareness materials should be provided to all staff with responsibility for records and should be customized for the type of User. The following is an example of the different types of training which may be offered:

Staff Category	Time	Example of Topics Covered
New Employee Orientation	15 – 20 mins – part of on-boarding	- Provide RIS Welcome Package - Identify contacts – who to contact for help or more information - Schedule follow up in 3 weeks after hire date to conduct more in-depth training at that time.
EDRM Basics	30 minutes	- RM benefits & need for compliance - EDRM responsibilities - ARCS/ORCS Overview

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

Staff Category	Time	Example of Topics Covered
		- EDRM System Overview/Where to Store? - Navigating, Searching, Adding, Revising Content
EDRM Advanced – Department Specific Content	1 hour	- RM benefits & need for compliance - EDRM responsibilities - ARCS/ORCS Overview - EDRM System Overview/Where to Store? - Navigating, Searching, Adding, Revising Content - Collection specific naming conventions, metadata, workflows as needed
EDRM Administrative Support - Department Specific Content	1.5 hours	- RM benefits & need for compliance - EDRM responsibilities - ARCS/ORCS Overview - EDRM System Overview/Where to Store? - Navigating, Searching, Adding, Revising Content - Collection specific naming conventions, metadata, workflows as needed - Granting permissions, understanding security classifications

4.1.2.4 EDRM Program Assessment Process

Following the implementation of the recommendations for user training and support, it is recommended that the Commission develops and deploys an EDRM Program assessment process. The EDRM Program Assessment will act to monitor success of, and adherence to the EDRM component of the Records Management Program and to identify and minimize the organization's exposure to risks inherent in the future management of large decentralized collections of electronic records using the new EDRM tool. The assessment will provide a baseline on user adoption and compliance and is a proactive approach to continuous process improvements.

The purpose of an assessment process is:

- Provide information about the efficiency and effectiveness of the EDRM Program as a whole and of the individual procedures that make up the program;
- Measure accuracy and adherence to program standards;
- Highlight problem areas; and
- Provide a basis for corrective action of both department practices and the EDRM Program itself.

NTT DATA recommends that the Commission's EDRM Program assessment consist of the following three components:

- Periodic Department Assessments
- Annual Department Assessments

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

- Program Assessments

Periodic department assessments can be conducted bi-annually or more frequently if necessary and Department and Program assessments conducted annually. User surveys, checklists and examinations of files and electronic environments (as some examples) are methods that can be used to complete the assessment. At all times, the Assessments must be objective, measurable, and used as opportunities to support and assist the Departments to better manage their information. The Assessment Program and details of the scope and measures should be shared with Department Managers and Administrative Support Staff once they are finalized and prior to conducting an Assessment.

4.1.3 Summary – Records Management Governance

The following summarizes the recommendations within the Records Management Governance Component as it relates to EDRM at the Commission:

- Establishment of a dedicated EDRM resource person
- Explicit Identification of EDRM Responsibilities for all staff as applicable
- Review and development of EDRM Procedures and Best Practices
- Development of EDRM Training and Awareness Program
- Development of EDRM Program Assessment Process

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.2 Records Classification and Retention Schedule

The Commission's records management program is built largely around the ORCS and ARCS, which categorizes records by subject or activity and defines how long records are to be stored before they are destroyed in compliance with applicable laws, regulations and other business requirements. The Commission adopted ORCS and ARCS upon its inception in 1998 through inherited collections of records from existing Ministries and continues to update its ORCS to address unscheduled and/or new business areas and activities.

ISO 15489 explains some of the main features of a compliant Records Classification and Retention Schedule:

- Organizing records according to the business activities of which they provide legal evidence
- Providing a conceptual basis for the reliable retrieval of records
- Assigning responsibility for particular sets of records to appropriate groups within the organization
- Establishing records retention periods and appropriate methods of final disposal and/or storage

In assessing the Commission's compliance with this Component, with focus on its unstructured electronic records, the Project Team explored three main issues:

- Degree to which each Department had successfully applied the Records Classification and Retention Schedule to its business records;
- Whether various content elements within the classification (categories, headings, scope notes, responsible departments) still accurately provided for the business functions, activities, and records of the office; and
- Whether records retention periods still provided for the operational needs or known legal/regulatory requirements for keeping records.

4.2.1 Findings – Records Classification & Retention Scheduling

Success levels in applying and implementing the Records Classification and Retention Schedules varied across different offices and Branches. Some areas have applied ARCS/ORCS to both hard copy and electronic documents while others have not implemented the system at all.

The overall compliance levels under the Component of Records Classification and Retention Scheduling as it relates to unstructured electronic records were as follows:

Records Classification & Retention Scheduling	**52% - Level 3 (Essential)**

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.2.1.1 ORCS Update Phase 1 - Completed

As a Phase 1 initiative, ORCS was re-developed as required under the IMA legislation and deemed essential for the appropriate management of Commission records. Approved for use in 2019, ORCS forms the operational framework and modernizes the original ORCS to current standards and positions the Commission to become EDRM ready. Phase 1 was designed to apply classifications and retentions to most Commission operational program records saved on the network. Those records remaining will be addressed in ORCS Phase 2.

4.2.1.2 ORCS Update Phase 2

ORCS Phase 2 commenced in fiscal 2020/21 and involves a detailed analysis of all Commission systems holding operational data and records. The Commission has a complex and ever-changing system environment. New systems are being initiated on a continual basis. A review of each operation system is necessary for ensuring IM compliance and retention planning has been addressed. As a Phase 2 initiative, existing approved records schedules (ARCS, Human Resource ARCS Supplement - HRAS) will be assessed for suitability for the Commission's administrative records with the potential of creating new customized schedules to address record retention needs.

ORCS Phase 2 development is required under the IMA legislation and necessary for the appropriate management of Commission data and records. Phase 2 is ongoing and recognized as a long-term initiative.

4.2.1.3 Unstructured Electronic Records

The Commission's shared drives (e.g. K: Drive) and Outlook (email) are being used as an unstructured recordkeeping system throughout all offices and Branches. The challenge is steadily increasing as more records are created and received. Information related to and supporting business functions is fragmented and staff experience difficulty locating records needed for their work or may not have access to the information they need for decision-making purposes. A summary of risks operating in this type of information environment may be summarized as follows:

- Inability to locate critical information;
- Non-compliance with applicable IMA and FOIPPA legislation, policy and best practices;
- Destroying records before they are legally eligible for destruction (not keeping records long enough);
- Keeping records longer than required thus creating risks associated with FOIPPA and document production under litigation (e.g. having to produce records that legally could/should have been destroyed);
- Mixing transitory information with official records; and
- Lack of protection for personal and/or sensitive confidential information.

Management recognized the need for appropriate classification and reorganization of electronic records to address these issues as well as for future EDRM implementation. Commenced in 2018/2019, a contract was initiated with a RIM consulting company to organize shared drive records according to ARCS/ORCS on a program-by-program basis. This critical work was paused for 2020/21 due to the uncertainties associated with Covid 19 and is resuming for fiscal 2021/22.

4.2.1.4 Records Searches

Another major finding is that the Commission does not currently use an automated records management system. There is currently no ability to search or index records across the organization. The Commission

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

must routinely respond to time-sensitive FOIPPA requests, and requests for records by counsel and in response to litigation. Not having these records indexed makes it difficult to respond in a timely manner. The RIS Branch FOIPPA Specialist(s) works collaboratively with all levels of staff on FOIPPA requests, and with Legal Services to support their requirements.

Conducting adequate and thorough searches for records across the Commission can be challenging due to the fragmented, siloed and unstructured state of its records. A typical request involves searching multiple repositories, systems and information locations and there is a real risk that not all information is being located/produced.

In an organization the size of the Commission, the task of effectively and efficiently managing and controlling records without automated tools such as an EDRMS is extremely difficult if not impossible, and creates the following situations:

- Difficult and time consuming to determine the ownership, location or existence of records;
- Decreased decision-making ability due to inefficient access to information resources;
- Increased storage and retrieval costs because content is not tracked and indexed;
- Unnecessary labour costs to perform easily automated manual tasks such as transferring files offsite and creating file listings; and
- Overwhelming difficulties enforcing legislative responsibilities and consistent record keeping practices.

Having records identified incorrectly or not identified at all increases the risk of not being able to find information, loss of credibility as a public institution and obvious time wasted searching for records.

4.2.2 Recommendations - Records Classification & Retention Scheduling

4.2.2.1 Shared Drive Implementation Plan

Already a key part of the existing RIS branch EDRM readiness plan, it is recommended that the Commission continue with the ongoing classification of electronic program records. This work is of high value to the Commission. Most of the program records are considered critical collections and an organized shared drive is not only foundational preparation for a future EDRM project, but key to securing and protecting the Commission’s information assets over the long term.

It is further recommended that the Commission take a more direct and focused approach within all areas to organize shared drives as a whole. Currently, the Commission approaches shared drive projects with a two-pronged approach: “do-it-yourself" (DIY) projects completed by program staff with guidance from RIS branch; and a series of formal guided projects lead by the contracted RIM consultant. I

When the Commission initiated its shared drive organization project in 2017/18, it was decided that Human Resources would serve as the pilot area. Since then, a systematic approach to folder cleanup, organization, and classification structure has been applied to each subsequent program area. Selection of areas has been ad hoc, based on operational cycles and client readiness. To date, the Commission has completed a total of six projects with the RIM consultant with a seventh project underway.

It is recommended that a comprehensive Shared Drive Implementation Plan be initiated to drive the cleanup of all network directories. An Implementation Plan may serve to formalize the process and communicate the benefits of the work across the organization.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

A Shared Drive Implementation Plan involves the purging and restructuring of shared electronic directories within the MS Windows environment. The benefits of cleaning up network drives are as follows:

- Organizes collections of active records that reflect individual department responsibilities and accountabilities;
- Removal of outdated and redundant documents no longer needed;
- Addresses and secures a home for the “orphaned” content;
- Supports compliance and reduces risk;
- Increases efficiency when locating information;
- Facilitates information sharing and collaborations; and
- Readiness of critical document collections for conversion to more advanced document management technologies.

The recommended approach is to start with a Pilot area to demonstrate the concepts and folder design principles for the Pilot Department shared drive. Although similar in design, each Department will require an electronic folder structure customized for their particular content. The Program records cleanup will augment this initiative. The objective is to have consistent, compliant practices within each business area.

As a minimum, the Shared Drive Implementation Plan should include the following elements:

- Enrollment - introduce the Branch in the initiative and agree on a timeline / schedule for completion
- Content Analysis - Existing shared drive folders, directory tree structures, program structures (existing)
- Design - Drafting suggested new folder structures/sub structures
- New Environment Set Up - Establish new folder structures for the Branch in their existing directories
- Training – Offer workshops, deskside support and User documentation on naming standards, folder design principles and best practices for using an electronic shared environment
- Support - Regular monitoring of progress of clean up and assistance as needed

4.2.2.2 Records Searches

As part of this initiative, business requirements have been identified to address functionality for an EDRM system which includes tracking and control of record holdings to support records searches. See Appendix B.

4.2.3 Summary – Records Classification and Retention Scheduling

The following summarizes the recommendations within the Records Classification and Retention Scheduling component of records and information management at the Commission:

- Shared Drive Implementation Plan
- Implementation of an Electronic Document and Records Management (EDRM) system to support records searches

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.3 Electronic Records Management

British Columbia, along with most legal jurisdictions, defines a 'record' as recorded information in any medium or format. As such, legal definitions do not distinguish between paper and electronic records, therefore organizations must apply the same records management standards to their electronic information systems as to their paper files. However electronic recordkeeping does introduce new challenges which warrant special attention in this report. In assessing how well the Commission responded to these challenges, NTT DATA explored the following questions:

- Are computer drives, folders and other such structures organized according to a standardized taxonomy which assists in compliance with ARCS/ORCS and allows staff to find records and information to support their activities?
- Are emails managed and retained according to Commission records management policies?
- Are strategies in place to minimize the duplication of information, in terms of both multiple electronic records and between paper and electronic versions?
- Does the Commission have a version control procedure or tools to help identify when a document becomes an official record?
- Are digital images of paper records created according to a controlled process which ensures the reliability of the image as a substitute for the original?

4.3.1 Findings – Electronic Records Management

To date, the Commission has made limited progress in systematically applying ARCS/ORCS to the Program records, documents and data created and stored on electronic systems. Outside of the Commission's operational information systems, there is heavy reliance on shared drives as recordkeeping repositories. Additional concerns with respect to electronic document management dealt with the management of data contained on email and personal computing devices.

Coming in with the lowest overall rating for the Commission, compliance levels under this Component are as follows:

Electronic Records Management	**13% - Level 1 (sub-standard)**

4.3.1.1 Reliance on Shared Drives

Electronic business documents are stored primarily on shared drives. As noted, the RIS Branch has engaged a RIM consultant and supported several Program areas in developing and implementing electronic folder structures that mirror the ARCS/ORCS classification structure. Once complete, adherence and ongoing maintenance of these folder structures is left to individual and/or department practices. Overall IT network administrators provides access and security to these electronic folder collections. The Windows environment does not have version control or document sharing capabilities.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

The electronic records at the Commission are not subject to automated removal for inactive storage or deletion. While network backups are handled on a regular basis, the contents of the network drives or data contained within software applications are not being managed from a records management standpoint.

With no centralized control or tools for applying standards, users across the organization have encountered challenges with redundant copies, competing versions, and difficulty locating information due to inconsistent naming conventions and personalized folder structures.

Long term management and ongoing preservation of scanned records is also an issue. The Commission routinely converts high volumes of hardcopy records held in historical asset and application files (e.g. well, pipeline, facility and associated application files, as well as other ancillary applications) to digital format for internal and external client use. For some records, their provision is a legal obligation under the Oil and Gas Activities (OGAA) General Regulation and forms part of the Commission's mandate. Digital copies of scanned historical asset records are included amongst the electronic records saved on shared drives.

4.3.1.2 Email Management

The Commission, like many organizations, experiences inconsistent business e-mail management practices across the organization. The Commission currently limits the size/amount of employee e-mails. Some business areas delete emails to comply with the size limitations while others are letting messages aggregate uncontrollably inside their MS Outlook e-mail environments.

4.3.2 Recommendations – Electronic Records Management

4.3.2.1 Continue Organizing Shared Drives

NTT DATA recommends that the Commission continue its work in implementing the shared drive reorganization process as described in the previous section 4.2.2.1. Standard folder structures and naming conventions for the storage of electronic information should be designed in parallel with the ARCS/ORCS structure and applied for all records in every program and business areas. The stretch goal is to have all Commission electronic documents, program and administrative related, fully classified and naming conventions applied prior to migration to EDRM.

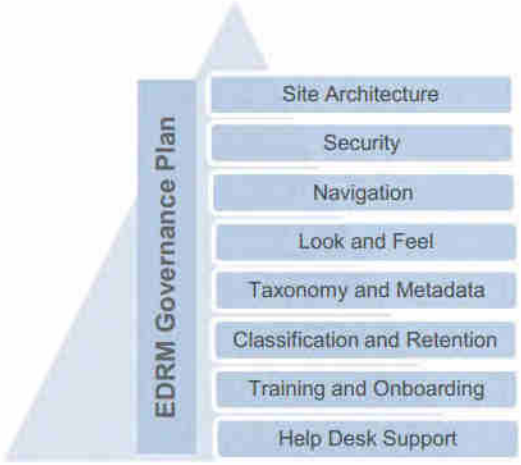
4.3.2.2 Develop An Electronic Content Management Strategy

Once the shared drive reorganization process has progressed, the Commission will be well positioned for implementation of an Electronic Document Records Management (EDRM) system. EDRM encompasses the management of electronic records, documents and e-mail, including version control, security and authenticity assurance. These tools are not a solution in themselves – and RIS, IT and Users need to remember that the proper application of records management principles along with building well-designed structural elements will ensure the success of any system adopted.

One of the basic components of any EDRM strategy is the Records Classification and Retention Schedule scheme. Once information is migrated to an EDRM platform, electronic document collections can be 'tagged' and meta data applied such as retention code, department name, etc. that will allow for more robust information reporting, management and searching. However, whether information is stored electronically or in paper, tracked manually or with advanced document management technologies, the same principles of organization, consistency and control must be applied.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

While the technical functionality of these systems is important, the application, design and deployment of the software are vital to its acceptance, use and control by the business areas. NTT DATA recommends the development of an EDRM Governance Plan to establish minimum rules of engagement, procedures and guidelines related to the use and administration of the EDRM system which would address the following general areas:



It is further recommended that any system be piloted on a small collection to evaluate the usability of the system and to identify any issues to be addressed prior to full implementation.

As part of this initiative, business requirements have been identified to address functionality for an EDRM system. See Appendix B.

4.3.2.3 Apply E-Mail Best Practices

Enterprise email management systems are part of an overall solution and are interdependent with the Commission's EDRM strategy which will address automated email archiving. Until these tools are available, it puts undue pressure on individual employees to manually process and organize the increasing volume of email back log.

Following the implementation of EDRM and the associated email management solution, email messages can be migrated to appropriate electronic records storage locations within the EDRM system. As a result, the messages would become available for access / sharing across a team or business area yet still would be managed by automated records governance rules of classification and retention.

The RIS branch is developing an email management guide to support staff in email management best practices. Currently, recommended records management practices involve deleting transitory emails and filing official email records to applicable shared drive recordkeeping systems.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

As an interim step, NTT DATA recommends that RIS raise the awareness of email best practices such as definition of business emails, proper use of Subject Lines, handling attachments, saving emails to the network, creation of folder structures within Outlook, sender's responsibilities for saving, management of inbox traffic, deletion of non-business and transitory emails, etc. The principals and practices for properly managing emails will continue to apply with or without an email management solution.

4.3.3 Summary – Electronic Document Management

The following summarizes the recommendations within the Electronic Document Management Component of records and information management at Commission:

- Continue Organizing Shared Drives
- Develop An Electronic Content Management Strategy
- Apply Email Best Practices

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.4 Information Protection

The component of Information Protection refers to a wide range of storage devices and facility features that help protect computing devices, paper and other records media from loss, damage and unauthorized access. Such measures support the other four RM Components of Compliance by ensuring that records are kept accessible, confidential and reliable for as long as business dictates. In assessing the Commission's compliance within this Component, NTT DATA addressed questions such as:

- Are you aware of or familiar with any disaster recovery or business continuity plans?
- Are paper files and other media stored in enclosures and/or facilities which prevent access by unauthorized persons?
- Are offices and records storage areas equipped to mitigate the risks of loss or damage due to fire, floods and other emergency situations?
- Are records of long-term value sufficiently protected against environmental degradation and user wear and tear?

4.4.1 Findings – Information Protection

Facilities and practices related to Information Protection scored the highest of all components surveyed. Overall compliance with this Component were as follows:

Information Protection	**83% - Level 5 (Transformational)**

4.4.1.1 Business Continuity Plan and Vital Records

At this time, there is a documented Business Continuity Program (BCP) for the Commission and vital records have been identified within the context of this plan. Communication with Program areas as to the identification and protection measures required for vital records come under the purview of the BCP Director.

As stipulated in the BC Government's Core Policies and Procedures for Information Management and Information Technology Management, the following are requirements relating to vital records and information technology business continuity plans:

- Government must create and maintain a business continuity plan that includes identification and management of its vital records.
- Vital records must be maintained so that re-establishing the legal, financial and functional responsibilities of government is achieved quickly after a catastrophic event or crisis.
- Vital records must be maintained in a manner that meets current environmental and security standards.
- Ministries must develop, or work with their supporting infrastructure technology service providers to develop Business Continuity and Disaster Recovery Plans on all information systems and the associated technology infrastructure and test them regularly.

Repercussions arising from the inability to recreate vital records may include the following:

- Reduction or loss of financial revenue;

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

- Reduction or loss of organizational productivity, including creation and provision of goods and/or services;
- Disruption in customer service;
- Increased exposure and vulnerability to litigation-related factors, such as lawsuits and legal penalties;
- Reputational damage; and
- Unexpected administrative and other financial expenses.

Vital records within the Commission have been identified, and include well files, pipeline files, application files, facility files, pay and financial records. The centralized records centre in Fort St. John holds the physical copies of these records (well, facility, application and pipeline files) and older financial and legal records are maintained in government contracted storage facilities. These facilities were purpose built for this function, with fire suppression and safety measures in place. Electronic records considered vital are protected by IT through regular network or system back up processes.

4.4.1.2 Information Security Classification

The provincial Information Security Classification Standard provides a common standard for security classification of government information. As shown in the following table, this standard describes four levels of security classification to be applied to government information based on the degree of harm that could reasonably be expected to result from unauthorized disclosure.

Within IT, network security and permissions are handled by controlling access to specific network resources, shared drives, systems or applications for individual users or groups. Information security is handled on a per system basis.

	Level	Description
PUBLIC		No harm to an individual, organization or government Examples: Job postings, communications to claim clerks, business contact information, research and background papers (without copyright restrictions)
CONFIDENTIAL	Protected A	Harm to an individual, organization or government Examples: Home addresses, dates of birth, other low-risk personal information
	Protected B	Serious harm to an individual, organization or government Examples: Law enforcement and medical records, personnel evaluations and investigations, financial records, information subject to solicitor-client privilege or other legal privilege
	Protected C	Extremely grave harm to an individual, organization or government Examples: Information about police agents and other informants, Cabinet records or Cabinet-related records

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.4.2 Recommendations – Information Protection

4.4.2.1 Strategy for Vital Electronic Records Protection

An EDRMS will support the protection of vital electronic records. The Commission has sound protections in place for its physical vital record holdings, however it also needs to protect the authenticity, integrity and stability of the electronic vital records. Appropriately storing electronic vital records ensures they are backed up on a secure storage device and the Commission can be assured that the vital records holdings within their custody are safely protected for generations to come.

4.4.2.2 Adoption of Security Classifications

Within the context of EDRM Governance Plan described in Section 4.3.2.2, the recommended security classifications must be adopted and applied to content migrated to this system. As part of an overall Security governance model, mandatory metadata such as security roles and confidential classifications of data elements will ensure the protection of confidential information across all business areas.

4.4.3 Summary – Information Protection

The following summarizes the recommendations within the Information Protection Component of records and information management at the Commission:

- Strategy for Vital Records Protection
- Adoption of Security Classification

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

4.5 Information Flow and Retrieval

The Component of Information Flow and Retrieval encapsulates a number of practical needs that an organization must address in order to comply with requirements and manage its business more efficiently. Among the key criteria assessed under this Component were:

- Overall assurance of timely access to and retrieval of records needed for daily business decision-making;
- Ensuring that records are accessible only to those who have a genuine need to access that information for purposes of completing authorized activities, as mandated by privacy laws and proprietary business rules;
- Minimizing storage costs and retrieval time by transferring inactive records to a more cost-effective location; and
- Ensuring that all relevant records, both active and inactive, will be located and retrieved in the event of a litigation, audit or personal information access request under applicable laws.

4.5.1 Findings – Information Flow and Retrieval

Rating in the Component of Information Flow and Retrieval varied greatly between Departments. Overall compliance levels under this Component were as follows:

Information Flow and Retrieval	**55% - Level 3 (Essential)**

While the Commission lacks some of the formal tools for managing records throughout the different stages of their lifecycle, some areas have achieved an adequate degree of control over active and inactive records. Within the Component of Information Flow and Retrieval, NTT DATA noted the following key areas for improvement:

4.5.1.1 Information Silos and Fragmentation

Clear interdependencies are well supported, but siloed information exists as a product of the separate and distinct systems and personal work habits (e.g. outlook, personal drives, unmanaged shared drives). Disjointed records collections make it difficult to manage the information within context of the whole and makes retrieval and identification of file contents inaccurate and inconsistent. This condition exists in both hard copy and electronic environments.

Major records streams are fairly consistent and therefore easier to access (supported by centralized file rooms for physical records and systems for digital information). Outside of the main program areas or when searching for information outside of the User's home Department, siloed information practices present challenges in locating records.

4.5.1.2 Records Searching

It is difficult for the RIS staff to do basic record searches and retrievals with confidence. RIS Branch staff face a complicated, multi-step process for searching, locating and retrieving active and offsite records. Multiple versions of excel tracking spreadsheets are maintained by the records management staff for locating offsite records and there is heavy reliance on records staff to interpret data contained within the

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

multiple spreadsheets and locate records. There is a risk when responsive records must be produced within rigid time limits for FOIPPA or litigation, and it is not clear that all information has been located.

4.5.1.3 Unmanaged Working Files

Users tend to create Working files for cross-functional activities such as projects, proposals, draft legislation, etc. For the most part, these interim files are not entered or tracked anywhere within ARCS/ORCS making it difficult to search for the location of information before close out or completion of the project or activity. While not a concern for many short-term activities, it does create difficulties with files created for long term projects or strategic developments and increases the risk on not being able to find required records in a timely manner. As well, the shared drive has no version control abilities, so it is very difficult to identify and control the latest and most complete versions of documentation.

4.5.2 Recommendations – Information Flow and Retrieval

The Commission should take the following steps to better control the flow of information and support overall business efficiency:

4.5.2.1 Content Mapping for Critical Collections

To address fragmentation and file integrity issues across the Commission for critical collections, NTT DATA recommends that Commission initiate the identification and documentation of locations of file collections for each Program area. Information to be captured for each collection would include such details as:

- Official Title of Collection
- Owner / Custodian
- Naming Conventions / Indexing
- How Organized / Folder or Document Sub Structures / Taxonomies if any
- Document Types and media (h/c, electronic, system of record)
- Permissions
- Location(s)
- Retention Period

The organization and cleanup of electronic program records currently being conducted will greatly contribute to this initiative.

4.5.2.2 Working File Administration

For multi-departmental long-term projects and initiatives, encourage Users to manage their Working Files within an ARCS/ORCS structure and create a process to merge and purge Working Files following project completion and close out with the Project Lead. The management of working files will become much easier following the implementation of EDRM.

4.5.2.3 Offsite Records Tracking

The RIS Branch would benefit from a simple/searchable database that contains all key information related to the Commission's offsite record holdings, which an EDRM will provide. This will address access issues, reduce risk of non-compliance associated with records searches, and ensure accurate information related

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

to offsite record holdings is available. The requirements for this functionality are addressed in the EDRM business requirements found in Appendix B.

4.5.3 Summary – Information Flow and Retrieval

The following summarizes the recommendations within the Information Flow and Retrieval Component of records and information management at the Commission:

- Content Mapping For Critical Collections
- Working File Administration
- Offsite Records Tracking

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

5 EDRM System Business Requirements

EDRM encompasses the management of electronic records, physical documents and e-mail, including version control, security and authenticity assurance. One of the basic components of any EDRM strategy is the Records Classification and Retention Schedule scheme. Once information is migrated to an EDRM platform, electronic document collections can be 'tagged' and metadata applied such as retention code, department name, location, etc. that will allow for more robust and secure information reporting, management and searching.

Guiding principles for the selection of an EDRM system include:

User Friendly – To support high user adoption, the EDRM system must be logical to operate and simple to learn. The interface must be consistent across all windows, menus, functions and commands. It must be intuitive to navigate and search, with as few mouse clicks and keystrokes as possible. It must also be accessible both on the desktop and in a web browser.

Classification Inheritance – The EDRM system must have the ability to automatically capture and apply records classifications to content in the background, without infringing on usability for end users. In essence, it must allow users to manage and store their information in the EDRM repository in a way that is meaningful and aligned to their business process and practice, while the system captures and classifies it in the background.

Robust Security and Audit Capabilities - The system should allow for varying levels of access, where sensitive, private or classified information can be restricted so that only specific individuals within the Commission can view or use it. The EDRM system should always prevent the unauthorized destruction or deletion of registered physical and digital records and associated metadata. The system must also provide audit trails of who had access and the actions taken on the records.

Manage Electronic, Physical and Hybrid Records – The EDRM system must be able to manage physical files as well as electronic records. These functionalities enable the management of the physical location of records in the form of paper files, tapes, disks, reports and archive boxes, and their storage locations, which may include filing cabinets, offsite commercial storage locations, and archival repositories.

Implementing EDRM within the Commission will not only to make it easier to locate documents and records, but also for future document control and advanced record management practices. EDRM software solutions integrate all current business document management into one seamless, centralized electronic records system.

EDRM System Business Requirements are detailed in Appendix B.

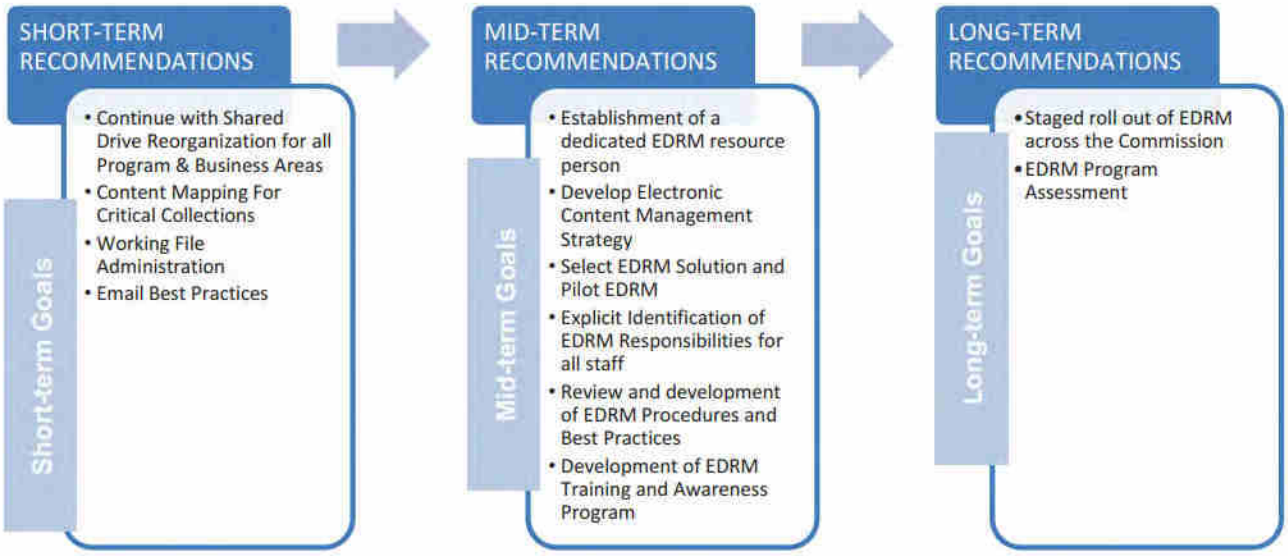
© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

6 EDRM Road Map

The recommendations that are presented in this report should be considered as pieces belonging to an overall Commission EDRM deployment strategy. The overall prioritization and execution of changes to how information is being handled must be driven by an integrated, comprehensive and well supported plan much more encompassing than what was included in this study.

NTT DATA acknowledges the Commission already has in place many components of a comprehensive Records Management Program however, it is important for the Commission to consider the actions outlined below in order to obtain a fully compliant EDRM Program as they move into an increasingly complex electronic information management environment.

The following summarizes the suggested priorities and time frames for the implementation of recommendations to mitigate risk in the most optimized manner in terms of short-, mid-, and long-term goals.



© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

7 Conclusion

NTT DATA's EDRMS Needs Assessment examined different facets of the Commission's tools and practices for managing its electronic records. The assessment found that while the Commission already has many key foundational practices in place, there are several important actions to take or continue before its records can fully support business efficiency and manage operational risks across the organization.

Implementation of an EDRM system to store and preserve its critical administrative and operational records collections, supported by the continued cleanup and reorganization of shared drives are strategic measures for advancing information management practices at the Commission.

While applying these recommendations is a significant task, doing so will bring tremendous return-on-investment in the form of improved business efficiency, legal and operation risk management, and accountability. NTT DATA is always pleased to provide further information and welcomes further opportunities to partner with the Commission in realizing these benefits.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

8 Acknowledgements

NTT DATA would like to graciously thank Kathryn Smerechinskiy, Rob Smith, Mahia Frost and Dana Keough for their support and guidance throughout this project. NTT DATA is proud to partner with the Commission to support their records management initiatives and looks forward to continuing the successful relationship as they grow and expand their records management program.

© 2021 NTT DATA, Inc. | All rights reserved. | Proprietary and Confidential | April 30, 2021

Records & Information Services (RIS) Branch Planning for Fiscal 2024/25

Summary of Key FOIPPA and Records Management Issues, Risks & Gaps to Assess Project Priorities & Resource/Funding Requirements

March 27, 2024

Table of Contents

EDRMS READINESS

1. ORCS Development – Phase 2: Creation of System Overviews & Assessment of Program Areas for ARCS Applicability
2. Organization/Clean-Up of Electronic Program Records on Shared Drive(s) in Accordance with ARCS/ORCS

DATA DEFRAGMENTATION STRATEGY - DIGITIZATION

3. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem: Creation of Data Source Roadmap to Identify Locations of Relevant Well Data/Records
4. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem: Conversion of Pre-2014 Records from Hardcopy to Electronic Format
5. Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem - Risk of Legislative Non-Compliance: Well Log Records
6. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem - Risk of Legislative Non-Compliance: Pressure Test Records
7. Conversion of Hardcopy Field & Pool Files to Electronic Format - Digitizing Key Record Series Maintained/Utilized by Reservoir Engineering & Geology Staff

FILE INTEGRITY

8. External Release/Publication of Well Information: Appropriate Management of the Two Sets of Well Files Maintained by Victoria and FSJ Offices

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
Foundational Elements / EDRMS Readiness									
1		**ORCS Development – Phase 2:** **Creation of System Overviews & Assessment of Program Areas for ARCS Applicability**	• ORCS Phase 2 will involve: – Detailed analysis of all Commission systems holding operational data and records. This enables identification of retention plans for structured data held in Commission information systems (as well as GIS data). – Addressing any gaps within the ORCS structure; the ORCS structure may change as a result of understanding how records are currently management within systems, or how they will be managed in the future – Assessing the suitability of existing approved records schedules (ARCS, HRAS) for the Commission's "administrative" records; the development of new customized schedules may be required to address record retention needs. Phase 1 was completed, and ORCS approved in 2019.	High	• The BCER has a complex and ever changing system environment – new systems are being initiated on a continual basis. A review of each operation system is necessary for ensuring IM compliance and retention planning has been addressed. System Overviews are a requirement of the ORCS structure and subject to the provincial approval process. • The ORCS only applies to Commission operational records. Administrative records also need to be appropriately addressed through the use of existing schedules or creation of customized Commission-specific ones. *Administrative records relate to: finance, building/property administration, business planning, Board materials, IT/IS activities, internal audit, HR, etc.*	• **Commence Phase 2 in Q4** of fiscal 2024/25 (secondment). • Phase 2 work is extensive and anticipated to require 1-2 years to complete.	1. ORCS Phase 2 development is required under the IMA legislation and appropriate for the appropriate management of Commission data and records within systems. 2. Appropriate classification and retention of Commission administrative records is necessary for EDRMS implementation.	Pending	Digital Information Management Specialist
2		**Organization/Clean-Up of Electronic Program Records on Shared Drive(s) in Accordance with ARCS/ORCS**	• Commission shared drives (e.g. K: Drive) and Outlook (email) are being used as recordkeeping systems • This is a Commission-wide problem – appropriate classification/reorganization of electronic records is necessary for future EDRMS / recordkeeping system implementation • Information related to and supporting business functions is fragmented – staff regularly experience difficulty locating records needed for their work or may not have access to the information they need	High	• Official BCER information is being inadequately managed – the problem is steadily increasing as more records are created and received. • Risks include: – Inability to locate critical information – Non-compliance with applicable IM legislation, policy and best practices	**Strategy, Contracted Resource & Funding ($) for Ongoing Services:** • Projects involve the classification and organization of electronic records in accordance with government's approved records schedule for such records.	1. Initiates a key foundational activity necessary for establishing a state of EDRMS readiness. 2. Addresses sensitive records (personal information). 3. Implementation activities will serve to test the suitability of classification	Ongoing	RIM Contractor (Michelle Barroca)) *With assistance from:* EDRMS Specialist BCER Branches IT/IS

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

DRAFT

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
					– Destroying records before they are legally eligible for destruction (not keeping records long enough) – Keeping records longer than required; this can create risks associated with FOI and document production under litigation (e.g. having to produce records that legally could/should have been destroyed) – Mixing transitory information with official records	• Ongoing/systematic implementation of the ORCS on a program-by-program basis across the BCER. • Contract has been initiated with RIM consulting company (FY Information Management). • Ongoing project – 19 branches successfully completed	structures (ARCS, ORCS or HRAS) and identify any scheduling gaps. 4. Supports informed decision-making by Commission staff through making information accessible.		
BData Defragmentation Strategy - Digitization									
3		**Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:** **Creation of Data Source Roadmap to Identify Locations of Relevant Well Data/Records**	• Update – should include the Field and Pool and Applications and Activities on the K drive • Upload to eLibrary - currently they go to FTP – DK now naming and putting on K drive into Applications and Activities structure. • Currently a person gets FTP data link for FSJ, and also an e_library – easier for client and creates a full record. • Well data/records exist in multiple locations and formats throughout the Commission: onsite in FSJ (paper files); offsite in storage (Victoria); staff emails/Outlook; systems/databases; K: Drive; other shared drives. • The data/records are highly fragmented and inaccessible to staff (and public). s.13 / s.17	High	s.13	**Create a Data Source Roadmap:** • Create a reference tool to identify all "places" where Commission well data is located; this will assist staff with locating information, and support planning of future projects • Engage with other key staff within Planning & Technology Division, who may be collecting similar data for related initiatives	1. Identifies/illustrates severity of current well data/records data fragmentation situation within Commission 2. Information will serve as the basis for corporate business planning/working towards solutions 3. Information sharing benefit - supports collaboration with other branches/key staff to ensure information accuracy/completeness	Initiated	RIS Branch FSJ Records/Permit Administration (Jody Sutherland) *With input from:* Planning & Technology Division (Strategic Initiatives, Business Intel)
4		**Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:** **Conversion of Pre-2014 Records from Hardcopy to Electronic Format**	Background: • In 2014, the Commission introduced new requirements and technology (eSubmission) for permit holders to submit well records in electronic format only. This business process change ended receipt of well file records in paper format and helped to resolve a paper records backlog issue. • Some digitization of pre-2014 well file records has been completed; approximately 500 boxes out of a total 5000 boxes of well files • Presently, one FTE is dedicated to digitizing paper well records (Well File Technician). **Issue 1: Legislative obligations under OGAA and Information Management Act (IMA) and the expectation of well data in digital format** • Under OGAA, the Commission is required to provide well data (non confidential wells) to the public upon request. • All data is requested in electronic format by internal and external clients. • New information management legislation in BC (IMA) will require government information be created and maintained in digital format only (exceptions to digitization requirements may be made on a case-by-case basis). **Issue 2: High volume of requests received for pre-2014 well data in electronic format – Slow response time to public requests** • The Commission converted to digital well submissions in 2014 (eSubmission); well data received prior to 2014 was predominantly received in paper format with some electronic data provided on CDs, diskettes. • FSJ office supports onsite scanning by the public; Victoria does not – all external requests for pre-2014 well data requires in house	High	• Defining corporate direction and a long term strategy for digitization will support appropriate planning, budgeting, resourcing and prioritization of supporting projects and activities. • Well file records are made available in digital format to external and internal requestors; paper is no longer the format of choice. The majority of the Commission's well data exists in paper format (approximately 4500 out of 5000 boxes of records have not yet been made digitally available). • Well records are severely fragmented – documentation is filed in separate files and geographical locations (e.g. PST records, well logs, etc.). The only way to efficiently integrate/combine the records is through electronic means. Interfiling "paper" is not a feasible option based on how the records are currently maintained. • BC's new legislation (IMA) may require the Commission to digitize its records over time, due to their FR (full retention) assessment by a provincial archivist. With such an assessment, the records will be permanently maintained by BC Archives. BC Archives is developing a digital archives for government records – in future, only records in electronic format will be accepted for permanent transfer from government to the Archives. Although the Commission will retain the majority of its	s.13 / s.17 **Option 1** s.13 / s.17	1. Establishes corporate direction and long-term vision for the Commission's management and publication of well data 2. Supports a digital environment and better access to information 3. Resolves current file integrity and OGAA compliance issues: (i) well file records are scattered across multiple locations; (ii) files deemed 'masters' are actually incomplete (missing key records); (iii) the Commission is not providing complete information to the public for decision-making purposes. 4. Supports intent of the new IMA that government records be created/received "digitally" 5. s.13 / s.17 6. Digitization positions the Commission to be able to destroy paper versions of records once a digital version of the file	Ongoing Option 3 in progress – ad hoc digitization of well files upon request	Well File Technician s.13 / s.17

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
			scanning. As noted above, scanning requests are managed by one FTE (Well File Technician). • The volume of well data requests is high and multiple requests are received weekly. • In addition to external requests from industry, RIS branch routinely responds to monthly ministry requests (land sale audit) and ad hoc internal requests (orphan site audits). • Public expectation is that the Commission will provide requested data quickly; this expectation, coupled with the fact that there is only one FTE providing the service, puts considerable and constant pressure on that one FTE. **Issue 3: Well data is fragmented throughout the Commission –** s.13 / s.17 **Issue 4: The eLibrary is being publicly advertised as the official source for Commission well data** • The eLibrary is described on the Commission's external website as the digital archive for oil and gas data. • Commission staff direct the public to the eLibrary as the Commission's official repository of electronic well file data. • To date, the eLibrary only includes the contents of the well files originating in Victoria; it does not include the contents of FSJ's hardcopy well files. *For additional information, please refer to Issue Number 16.* **Issue 5: An ad hoc approach to well file digitization** • There has been no master digitization "plan" applied to the scanning of Commission records. • Digitization is typically done in an ad hoc manner, in response to internal and external requests for specified well data. The requests 'drive' which records are selected for scanning. • When the Victoria office move was announced, effort was made to digitized the files that were stored in the onsite file room; approximately 50% were digitized before the move. • Only 10% of the Commission's total paper well files (Victoria files) have been converted to digital format to date (500 out of a total 5000 boxes of files). • When requests for older records are received, the files are retrieved from storage, converted to digital format, and uploaded into eLibrary.. • Commission well data is fragmented; it is located in multiple formats and locations. *For additional information, please refer to Issue Numbers 11 through 14.* **Issue 6: Long-term offsite storage of well file records is costly over time** • There are approximately 5000 boxes of well files stored in Victoria offsite records storage facilities • Cost for storage is $.58/box per month = $34,800 per year		records for a long period of time, some will eventually be eligible for transfer. • The Commission should have a plan for addressing the digitization requirement for well files that will meet legal requirements, and support their accessibility and long term preservation	Option 2: Outsource well file scanning to an external service provider through a multi-year service agreement. s.13 / s.17 Option 3: A combined approach that incorporates Options 1 & 2. s.13 / s.17 Summary of Items For Decision: 1. **Determine Which Files Should be Digitized:** (a) Digitize all well files over time; (b) Digitize select well files; or (c) Digitize well files upon request (status quo). 2. **Determine How Digitization Should Be Addressed:** (a) Use internal resources; (b) Outsource to contracted service provider; or (c) A combined approach of (a) and (b).	has been created – this would be subject to: – An approved ORCS authorizing the destruction – Ensuring the IT environment appropriately safeguards the digital records and supports their permanent preservation (e.g. upon implementation of an EDRMS) – Government digitization and Commission quality standards for the records have been met 7. Systematic destruction of the hardcopy well files, once digitized, would reduce the Commission's ongoing, long-term box storage costs: – Storage of 5000 boxes of well files costs $34,800 per year – Storage of 700 boxes of well logs costs $4,870 per year – **Total annual storage cost is $39,670 per year**		

DRAFT

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
			• Storage cost (assuming rates remain unchanged at $0.58 per box per month) to store these records boxes for another 25 years would cost the Commission approximately $991,750, as these records have a long-term retention requirement. • Under the ORCS, well file records are fully retained (essentially kept "forever", until the Commission no longer requires them)						
5		**Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem:** **Risk of Legislative Non-Compliance:** **Well Log Records** **Commission may not be releasing complete information on wells to the public** *Relates to need for long-term strategy to address well file digitization (Issue Number 10)*	• The Commission is required to make specified well data publicly available under the OGAA General Regulation. • There are approximately **700 boxes of well logs** stored at Iron Mountain records storage in Vancouver, BC; these records should be filed within the corresponding well file, but are not. • The logs were previously removed from FSJ's hardcopy well files due to onsite storage limitations (space-saving measure). • While it's possible that a significant percentage of these logs are duplicates of those contained within Victoria's hardcopy well files, this is unknown and cannot be verified unless a comparison is done: (1) to the paper log to the well file contents; or (2) to the digital logs that have been uploaded to eLibrary. • The box content lists that were completed identify the logs by a well authorization (WA) number. It's possible to retrieve the logs related to a specific WA; it is not possible, however, to determine from the lists the exact number of logs related to a specific WA. • The Commission (RIS Branch) previously initiated discussions for a potential digitization contract with a Vancouver-based scanning service provider (MicroCom Systems) for 150 boxes of well logs, however this contract did not proceed. Proceeding with any scanning contract is not recommended until a strategy has been determined – ideally, the separated logs should be compared against the file contents of the "master" well files to identify/destroy any duplicates prior to initiating scanning. • s.13 / s.17 (at the time MEMPR had the well files, and logs weren't used up in FSJ)	Med-High	• Incomplete files: If the logs are not duplicates of those currently filed within the corporate well files, it means a portion of Victoria's WA files are missing relevant data and therefore "incomplete" (data integrity issue). • Incomplete responses: This translates into an information request compliance issue, in that the Commission may not be releasing complete records in response to external requests, nor publishing complete WA data on eLibrary. The public is routinely directed to the eLibrary as the Commission's "official" well file data repository. • Non-compliance with OGAA General Regulation: In terms of requested information, this omission could put us in contravention of OGAA General Regulation (the Commission's requirement to make well data available to the public). Unlike the FSJ office, Victoria is not set up for public access/self-scanning – this means that the public relies on the Commission to fully satisfy requests for well data. • Ongoing cost for storage: Based on the current rate of $.58 per box per month, the annual storage cost for the 700 boxes of logs is approximately $4,870. It's estimated that the logs have been in offsite storage for approximately 7 years, hence $34,000 has been spent to date on storing what could be duplicate records.	s.13 / s.17 Initiate log reconciliation/digitization project after substantial amount (e.g. 40-50%) of well files have been digitized. The logs are believed to pertain to more historical (older) well files that have not yet been digitized. The RIS Branch has not yet digitized many of the historical files; focus has been directed more on recent files (those that were physically stored in the Victoria Records Centre). • At some point, the hardcopy logs need to be reconciled against the well files to determine what is an original versus a copy, or if the log is missing altogether • This comparison is best done against logs that are digitized and available in electronic format (within eLibrary); a "paper" to electronic comparison approach would be taken. • s.13 / s.17 • When a significant portion of the Commission's historical well files have been digitized and uploaded to eLibrary, the hardcopy logs could then be retrieved from storage and compared to the electronic versions. This work would be completed by the Victoria Well File Technician. • Duplicate logs would be destroyed. Logs missing from the uploaded data would be digitized and added. • The amended ORCS, once approved, will provide legal authority for the destruction of the paper well files (including logs) once digitized.	1. Addresses OGAA compliance issue 2. Addresses record format, accessibility, data fragmentation, and duplication issues 3. Supports the eventual reduction of offsite records storage costs over time 4. Supports Commission's move towards a digital records environment	On Hold	No resource to support s.13/s.17
12		**Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:** **Risk of Legislative Non-Compliance:** **Pressure Test Records** **Commission may not be releasing complete information on wells to the public** *Relates to need for long- term strategy to address well file digitization (Issue Number 10)*	• There are approximately 128 boxes of hardcopy Pressure Test documents currently located in offsite storage. • These documents were formerly filed within Field & Pool files when the records belonged to the Ministry; a retroactive decision was later made by the Commission to have the document filed in the well files. Document refiling work was never completed by the Commission. • The issue is that this data is now stored separately and not part of the official well file; as a result, the data is not available to Commission staff or the public in response to information requests. • The boxes of records in storage are listed by Field & Pool/Project type. With the current arrangement of the records, it would be a difficult, multi-step process to try to locate and retrieve Pressure Test documents related to a specific well.	Med- High	• This finding relates and contributes to the problem of the Commission's fragmented well data (file integrity issues); files regarded as 'master' files by the Commission are incomplete and missing key documents. s.13 / s.17 • It is not feasible to refile the paper documents into the master well files – a single box of Pressure Test records contains documents related to 100 or more well files. The hardcopy well files are all maintained in offsite storage –	**Funding ($) for External Scanning Services:** • Addressing these records through a digitization project is the recommended approach for resolving this issue – converting records from paper to electronic format will make them accessible to Commission staff and the public. It will also support our goal of trying to unify the records that pertains to each well. • Once the Commission's amended ORCS has received provincial approval, the Commission will be authorized to destroy the paper records once they've been digitized (subject to Executive approval) • This would be an appropriate project to outsource to a contracted service	1. Addresses OGAA compliance issue 2. Addresses record format, accessibility, data fragmentation issues 3. Supports the eventual reduction of offsite records storage costs over time 4. Supports Commission's move towards a digital records environment	s.13/s.17	Records Analyst

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
					refiling would require the storage company to retrieve 100 or so different boxes of well files for every one box of Pressure Test documents. Refiling would need to be done onsite at the storage facility; the Commission would need to provide a resource to work onsite.	provider such as BC Mail Plus, as the documents are originals and of a regular/standard size (8 ½ x 11). BC Mail Plus is able to retrieve specified boxes directly from storage, scan their contents, and manage the destruction process.			
13	DONE	**Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem:** Risk of Legislative Non-Compliance: Oil, Gas & Water Analysis Records **Commission may not be releasing complete information on wells to the public** *Relates to need for long-term strategy to address well file digitization (Issue Number 10)*	• There are approximately 21 boxes of hardcopy Oil, Gas & Water Analysis documents currently located in offsite storage. • These documents should have been previously filed into the applicable Well files – it's possible that the documents were either removed from the master files and never refiled, or never filed into the master files upon their receipt by the Ministry or Commission (e.g. the Commission may have "inherited" the problem). • The issue is that this data is not part of the official well file and, as a result, not being made available to Commission staff or the public in information requests. • As the boxes of records are inadequately listed, it is almost impossible to locate/retrieve analysis documents related to a specific well.	Med-High	• **Same as above** - This finding relates and contributes to the problem of the Commission's fragmented well data (file integrity issues); files regarded as "master" files by the Commission are incomplete and missing key documents. • Risks include: the Commission not meeting statutory obligations related to the release of well data; and, Commission staff, researchers, etc. not having access to all pertinent information for decision-making.	**Funding ($) for External Scanning Services:** • **Same as above** - Addressing these records through a digitization project is the recommended approach for resolving this issue – converting records from paper to electronic format will make them accessible to Commission staff and the public. It will also support our goal of trying to unify the records that pertains to each well. • Once the Commission's amended ORCS has received provincial approval, the Commission will be authorized to destroy the paper records once they've been digitized (subject to Executive approval) • This would be an appropriate project to outsource to a contracted service provider such as BC Mail Plus, as the documents are originals and of a regular/standard size (8 ½ x 11). BC Mail Plus is able to retrieve specified boxes directly from storage, scan their contents, and manage the destruction process	1. Addresses OGAA compliance issue 2. Addresses record format, accessibility, data fragmentation issues 3. Supports the eventual reduction of offsite records storage costs over time 4. Supports Commission's move towards a digital records environment	Completed in December 2021	Records Analyst
14		**Addressing Well Data Fragmentation - Records stored in Email/Staff Outlook Systems:** Well Exemption Records **Critical emails that document evidence of Commission exemption decisions are not accessible to key decision-makers**	• Engineering and Permit Administration/Adjudication staff require knowledge of any exemptions granted to operators • These records are not stored in a centralized location or system – most are stored within the Outlook (email) systems of individual staff • These records should be included as part of the Commission's activity files (well, facility, pipeline) in a centralized and shared location • Lack of access to these records has negatively impacted Commission business (e.g. compliance, investigation and enforcement activities)	High	• Key staff require knowledge of/access to exemption decisions to effectively do their work • Lack of access can (and has) result in the Commission making incorrect assessments or decisions, and/or being put in a position of "embarrassment" (e.g. there have been cases where the Commission was unaware of an exemption when dealing with an operator)	**Collaborative Project with IT/IS (Possible Technical Solution) and Permit Administration (Possible Resource/Project Assistance):** • Work with IT/IS to identify s.13 / s.17	1. Addresses OGAA compliance issue 2. Addresses record accessibility, data fragmentation issues 3. Supports informed business decisions	Initiated *** Preliminary discussion with IT/IS has occurred re identifying/testing possible technological approaches or solutions* *Process changed – engineering now uploading themselves. 600+ docs digitized and uploaded. Completed – October 2023*	No resource to support *Potential for assistance/ assignment to FSJ Resource Data Coordinator staff*
15		**Conversion of Hardcopy Field & Pool Files to Electronic Format**	• The Field & Pool files are another key records series currently maintained in hardcopy format. • The files were previously stored in onsite office space (Victoria Records Centre), but have since been boxed and moved to offsite	Medium	As noted, continuation of a paper filing system will be problematic for a number of reasons: • Files will have to be continuously retrieved from storage in order to do filing	**Dedicated Project Resource (RIS Branch Records Analyst):**	1. Digitization supports staff accessibility to information (Engineering & Geology) and proactive release, as appropriate	In Progress	Records Analyst *With assistance from:*

Commented [TS1]: Correct number of boxes is 10. The box number range is #11-21. Accession number 95-2703. In process of scanning & uploading to eLibrary.

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
		Digitizing Key Record Series Maintained/Utilized by Reservoir Engineering & Geology Staff	storage. Ongoing filing of paper documents will be required as long as no digital file version exists – paper filing can no longer be sustained in the current environment as it would require ongoing retrieval of records boxes from storage. There is no room for file expansion within the 94 boxes of records, nor will the storage facility support retrieving records for an ongoing 'active' filing system. • In addition to the 94 boxes, there are an additional 100 or more boxes of older Field & Pool records in offsite storage. • A Project Charter was developed for a Field & Pool record digitization project by RIS Branch with Reservoir Engineering approximately 2-3 years ago. RIS Branch is now fulfilling that former commitment. • Priorities are done – no asks for remaining offsite material. There is still work to be done but the critical elements are done and operational work is supported. Update – ST and MF		• Inter-filing into 'boxes' is difficult and will eventually lead to the need to re-box records as more documentation gets added to the files (limited expansion capabilities) • Technically we are not supposed to store 'active' records in offsite storage – frequent retrievals may result in offsite storage facility raising this issue • BC Government is going digital – as well as the Commission; an ongoing 'print and file' approach is not sustainable or in alignment with the direction of records management. • Longer term vision is to make some of the Field & Pool information publicly available (e.g. via eLibrary)	• In collaboration with program staff, RIS Branch established a new electronic filing structure on the K: drive for Field & Pool records (to support the digital transition to records management) • Project focus is on the 94 boxes of records that were previously stored in the Victoria Records Centre; boxes are being retrieved from offsite storage incrementally and file contents digitized. Approved naming conventions are being applied to scanned records, and records are being organized in accordance with the new e-filing structure. The records meet naming convention standards required for future uploading to IRIS/eLibrary • The Analyst is analyzing file contents in detail and addressing any noted file integrity issues. • Regular updates and engagement with the Reservoir Engineering team is occurring ensure input into project. • RIS Branch will assess the value/need of digitizing the older Field & Pool files located in storage in future; conversion to digital format may or may not be warranted.	2. Digitization supports a necessary program area shift to accept only "digital" record submissions 3. Once ORCS Phase 1 is approved, the Commission will be authorized to destroy the scanned/duplicate paper copies (reduces offsite storage costs) 4. The process is supporting necessary corrections at a file and document level, thus improving file quality and integrity (e.g. opportunity to address misfiled documents)		EDRMS Specialist Reservoir Eng Geology
File Integrity									
16		**External Release/Publication of Well Information:** **Appropriate Management of the Two Sets of Well Files Maintained by Victoria and FSJ Offices** *Relates to need for long-term strategy to address well file digitization (Item Number 10)*	• Two sets of hardcopy well files exist within the Commission. One set is located in Victoria (offsite storage), and the other in FSJ (File Room). There are different document types filed within these sets. Victoria's files include records related to pre-drilling and drilling data, whereas FSJ's files include records related to post-drilling activities. • When individuals request a copy of a well file, the type of records received is often dependent on the office to which the request is made. • A request that is received by/directed to the Well File Technician results in a release of records from the Victoria well file – records found in the 'sister' well file in FSJ are typically not included as part of the response (unless the WA file cannot be located in Victoria, or specific documents related to the FSJ file are requested). Likewise, requests/walk-ins to the FSJ office result in different records being provided to the public. • FSJ office supports public walk-ins and onsite scanning of well files by the public. Victoria does not support walk-ins for onsite file viewing; rather, requests are managed internally by the RIS Branch (Well File Technician) who retrieves the requested well files from offsite storage, scans the records, and uploads the information to eLibrary. The requester completes the registration process to obtain a userid for access to online viewing within eLibrary. • Not all records filed in the FSJ well files are releasable under FOIPPA (e.g. landowner and First Nations information is confidential). • Files are partially duplicated – Victoria is the "technical file" and FSJ the "field" file, but when FSJ received the only copy of a "completion report" they kept it so they do have some technical material that Victoria doesn't have.	Medium	• Different records are available for release to the public based on office location. • Only records found in the Victoria well files are currently published on eLibrary – as previously noted, eLibrary is often pointed to as the only "source" of records for a given well. • Some members of the public may not be aware of the two sets of files and difference between their contents. • OGAA General Regulation identifies the types of well data that should be available for release. The Commission also has a requirement to make information available for viewing or copying. This is being done by the two office locations for the files they have custody of/access to, but it is not necessarily being done as a 'coordinated' activity.	**Further Assessment Required:** • Review and compare contents of the FSJ and Victoria well files; create a "document" inventory to understand the differences. • Review statutory requirements of OGAA in terms of release. • Flag documents not subject to release under FOIPPA. • Review current business processes maintained within and between the two offices with respect to managing information requests. • Determine whether or not any of the records maintained in the FSJ files should be included with well data made available in eLibrary; if yes, think about possible strategy/business process to support need. • Solution may include enhancements to current technological platforms/systems, such as AMS, IRIS/Kermit, eSubmission, to support document uploading.	1. Improves RIS Branch understanding of Commission well file records and current records management processes 2. May identify service gaps and/or confirm OGAA compliance issue	Pending	RIS Branch Permit & Administration
Administrative Efficiency									
18		**Classification of Unscheduled Hardcopy Records in Storage:** **Portion of Records in Offsite Storage Require Classification/ Scheduling According to**	• Some records have been sent to offsite storage without being unclassified/unscheduled, as "miscellaneous ARCS & ORCS". • Others have not had final disposition applied. • This work will require time and analysis. • Some analysis – planned.	Low-Med	• The Commission may be holding onto records and paying for records to remain in storage longer than necessary • Records held in storage are subject to FOI and litigation	**Hold Until ORCS Development Phase 1 is Approved & RIM Project Priorities Established for 2019/20:** • As time and resources permits, review offsite record 'holds' and box content lists to identify those unscheduled; complete	1. Supports records lifecycle management 2. Potentially reduces scope of FOI or litigation related requirements 3. Could reduce offsite storage costs	On Hold	No resource to support *RIS Branch resources busy with other high priority projects*

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

DRAFT

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
		ARCS/ORCS to Support Application of Final Disposition				necessary steps to have retention applied so that final disposition can occur • Focus on 'quick wins'; identify/flag accessions that may require more in depth analysis and time to address			
19		**Improvement of Tools for Managing Offsite Records Holding** Current Tools for Managing/Locating Corporate Offsite Record Holdings are Inadequate	• Multiple versions of excel tracking spreadsheets are maintained by the records management staff for locating records. • RIS Branch staff face a complicated, multi-step process for searching, locating and retrieving records from offsite storage. • Data in Kermit is not entirely reliable in terms of the location of records – staff try to update when they come across inaccurate information.	Medium	• It is difficult for RIS Branch staff to do basic record searches and retrievals from storage with confidence – this is a risk when responsive records must be produced within rigid time limits for FOI or litigation. • There is heavy reliance on one staff (Records Analyst) to interpret data contained within the multiple spreadsheets and locate records.	**Funding ($) For External Services - Option of Small Dollar Contract to Complete Work in 2019/20:** • Branch would highly benefit from development of a simple/searchable database (e.g. Access database) that amalgamates/contains all key information related to the Commission's offsite record holdings	1. Addresses record accessibility, data fragmentation issues 2. Reduces risk of non-compliance associated with records searches	On Hold	Records Analyst IST Sr Bus Analyst With assistance from: Well Tech

New items from brainstorming/review session:

Disposition of Shared Drive FD Folders

SharePoint Projects

Scanner wearing out – Terri

Cancelled wells – boxed in numeric order, possibly 120 boxes, there is a spreadsheet of all of them by WA number. Mixed up files that are cancelled but also with land disturbance so land disturbance needs to go on the shelf. Cancelled need documented destruction. .

Waste Management Files – organized and put into order.

Space out the shelves better in FSJ Records Centre.

DRAFT

ISSUANCE: **Corporate Services Division**
Finance & Administration Department

APPROVED: **August 10, 2018**

1.0 GENERAL

1.1 Purpose

The BC Oil and Gas Commission (Commission) views information as an important and strategic asset that must be appropriately managed throughout its lifecycle according to legislated requirements. This policy details the roles, responsibilities and principles for the effective and compliant management of Commission records.

1.2 Background

The Commission is subject to the statutory requirements of the *Information Management Act* (IMA) which requires the digitization of non-digital records (subject to specific exemptions) and the use of appropriate information management systems.

1.3 Applicability

This policy applies to all records, regardless of format, that are created or received by the Commission and its employees in the course of their duties. It also applies to contractors, consultants and agents of the Commission who have access, custody or control of Commission records.

1.4 Authority

- *Information Management Act*
- *Interpretation Act*
- *Electronic Transactions Act*
- *Oil and Gas Activities Act*

1.5 Definitions

- **Active records** are records referred to frequently for daily business operations, or that need to be retained and easily accessible on site (if records exist in physical format).
- **Administrative records** support common organizational functions such as the management of facilities, property, finance, personnel, and information systems. These records are managed (classified and scheduled) in accordance with the government Administrative Records Classification System (ARCS).
- **Confidential records** contain information requiring protection against unauthorized access or disclosure. Records are classified as confidential based on a variety of requirements, including, but not limited to, policy or legislation. For example, the *Freedom of Information and Protection of Privacy Act* (FOIPPA) identifies exceptions to the disclosure of requested information. Examples of Commission confidential records include well data, where confidentiality periods apply as defined in the drilling and production regulations, and First Nations

consultations and draft agreements.

- **Digital (electronic) records** consist of information that is entered, created, manipulated and/or stored on digital media or storage devices, and includes:
  - Records that are born digital;
  - Digitized records (converted from non-digital format);
  - Unstructured data (e.g. documents); and
  - Structured data maintained within electronic systems.
- **Electronic Document and Records Management System (EDRMS)** is an integrated software system capable of managing both electronic and physical records through their life cycle in accordance with ARCS, ORCS and other approved records schedules.
- **Inactive records** are no longer required for ongoing business. These are records that are ready for final disposition or, in other words, records for which the scheduled active and semi-active retention periods have lapsed.
- **Information management** is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Operational records** relate to those mandated functions which are unique to a government public body, for which it is responsible for performing according to statute, regulation or policy. These records are described in an Operational Records Classification System (ORCS).
- **Records** include any recorded information created or received, and retained in the day to day operations of business. This covers "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise" as defined in the *Interpretation Act*.
- **Recordkeeping system** within a government office refers to a shared ARCS and ORCS based filing system in which official (non-transitory) records are organized, retained and disposed of according to approved record retention schedules. A recordkeeping system may consist of physical files in a file room, electronic folders and records saved on a shared drive, or an Electronic Document and Records Management System (EDRMS).
- **Retention schedule** provides a timetable for maintaining an organization's records. It governs the life cycle of a file from creation, through active use to inactive storage (when appropriate) to final destruction or their transfer to the custody and control of the Provincial Archives. The approved retention schedules for government records are defined in ARCS and ORCS and are applied throughout a records life cycle.
- **Semi-active records** are used only occasionally and do not need to be maintained in the office space of the Commission. While they still have value, they can be stored in economical, offsite storage facilities.
- **Transitory records** are records of temporary usefulness that are not an integral part of an administrative or operational record series. Transitory records are not required to meet statutory obligations or to sustain administrative or operational

functions. As with all records, they can exist in any format or medium (paper or electronic). These records are not regularly filed with official Commission records within filing systems.

2.0 PRINCIPLES OF INFORMATION MANAGEMENT

The Commission must manage its digital (electronic) and physical (hardcopy) records in accordance with legislated requirements and government-wide policies and standards for recordkeeping.

2.1 Access to Records

Records are a corporate asset and resource, and need to be accessible and shared by staff where appropriate. Access to sensitive or confidential records will be restricted to individuals whose duties require such access, in adherence with applicable information security classifications.

2.2 Duty to Document

Employees must create and maintain complete and accurate records sufficient to document evidence of their business activities, transactions, policy or decisions.

2.3 Digital (Electronic) Records

Records created or received in digital (electronic) format shall be treated as the authoritative records source and remain in digital (electronic) format. As both the Commission and BC government move to a digital recordkeeping environment, printing and filing records in hardcopy should be avoided where feasible. Physical records may be digitized and stored electronically as the authoritative source, provided government's digital conversion standards are met. Destruction of any physical records after their digitization must be approved and documented by the Commission's records management staff.

2.4 Recordkeeping

Program areas are responsible for maintaining a shared office recordkeeping system for official active records. Records form corporate memory and must be incorporated into the shared recordkeeping system upon creation or as soon as practical. Government legislation requires the filing and retention of records in accordance with approved government records classification and retention schedules.

2.5 Records Disposition

When records reach their inactive stage they are ready for final disposition review. Records management staff will carry out the review and determine whether records require further retention or disposal. Commission records are not to be destroyed or disposed of without approval from the designated Corporate Records Officer.

2.6 Records Storage

When records become semi-active they will be moved into the applicable records storage facility (physical records) or managed within a secure records environment (electronic records) as determined by the Corporate Records Officer or prescribed in the Commission's records management procedures.

3.0 RESPONSIBILITIES

3.1 Executive and management are responsible for:

- Cultivating an organization-wide culture that values records and information management;
- Enforcing policy and procedures for the proper collection, creation, storage, access, retention and disposal of information; and
- Ensuring proper levels of protection are applied to confidential information under their custody and or control.

3.2 Each employee is responsible for:

- Managing their records in accordance with appropriate records retention schedules, policies, procedures and best practices;
- Understanding, identifying and routinely disposing of transitory information created or received; and
- Protecting records in their custody or under their control from unauthorized disclosure, inadvertent loss or destruction.

3.3 Commission records management staff are responsible for:

- Delivering an efficient and effective Records Management Program that offers succinct processes, solutions, and records management strategies;
- Providing Commission-wide records retention schedule(s), data plans, policies, procedures and guidelines related to collection, creation, storage, access, retention and disposal of records;
- Assessing organizational training and resource support needs, and developing appropriate plans and materials to address these;
- Assisting in defining records management business requirements and integrating information management planning into systems, plans and budgets and;
- The approval of and secure disposal of records.

APPROVAL:

Paul Jeakins
Commissioner,
Chief Executive Officer

Len Dawes
Executive Vice President,
Chief Financial Officer

Ken Paulson
Executive Vice President,
Chief Operating Officer

Mayka Kennedy
Executive Vice President,
Chief Engineer

Trevor Swan
Executive Vice President,
Chief Legal and Regulatory Officer

Version Control:

Document Created	Aug-18	

Information Security Policy

Information Technology

ARC 100-00/200

Issuance: Corporate Services Division

Approved by Executive February 15, 2017

GENERAL

The OGC is the custodian of extensive information holdings and relies upon its information assets for fiscal, policy and program delivery initiatives. The management of public information requires government agencies to protect confidentiality, integrity and availability of the information assets in its care.

The Information Security Policy is based on the ISO 27002:2005 standard for information security management and conforms to the spirit of Chapter 12 of the Core Policy and Procedures manual. This standard provides a structured approach to identifying the broad spectrum of information security activities in the life-cycle of information systems. This Information Security Policy provides the framework necessary for the protection of Commission information and technology assets.

The policy incorporates a risk assessment approach to security by considering, business process and government service delivery implications and technological implications.

The risk assessment approach enables:

- Compliance with legislative and policy objectives;
- Cost-effective allocation of resources based on a risk assessment;
- Responsible governance of the Commission's information assets; and,
- Secure provision of electronic services.

The Information Security Policy includes a Glossary of key terms. Terms from existing policies are adopted where appropriate.

Introduction

Chapter 1 - Security Policy

Chapter 2 - Organizing Information Security

Chapter 3 - Asset Management

Chapter 4 - Human Resources Security

Chapter 5 - Physical and Environmental Security

Chapter 6 – Information Security Services

Chapter 7 - Access Control

Chapter 8 - Information Systems Development and Maintenance

Chapter 9 - Information Security Incident Management

Chapter 10 - Disaster Recovery & Business Continuity Management

Chapter 11 - Compliance

Glossary

Chapter 1 - Security Policy

The Information Security Policy establishes requirements to ensure that information security policies, processes and practices remain current as business needs evolve and technology changes.

The Senior Network Security Analyst is responsible for establishing, issuing and monitoring information security policies.

1.1 - Information Security Policy

a) Information Security Policy

The Information Security Policy (ISP) contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of Commission services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of Commission information assets through:

- Management and business processes that include and enable security processes;
- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining Disaster Recovery plans; and,
- Monitoring for compliance.

b) Compliance with BC CIO Information Security Policy

This policy follows and enhances the BC Government ISP. The Commission ISP can exceed but must not conflict with the baseline established by the BC Government Office of the Chief Information Officer's Information Security Policy.

1.2 - ISP Annual Review and Updating

a) Information Security Policy review

The Senior Network Security Analyst is responsible for reviewing information security policies, standards and guidelines on an annual basis. Policies and standards review must be initiated:

- In conjunction with legislative, regulatory or policy changes which have information management implications;
- During planning and implementation of new or significantly changed technology;
- Following a Security Threat and Risk Assessment of major initiatives (e.g., new information systems or contracting arrangements);
- When audit reports or security risk and controls reviews identify high risk exposures involving information systems;

1.2 - ISP Annual Review and Updating cont.

- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of investigation into information security incidents;
- Prior to renewing third party access agreements which involve major government programs or services;
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues; and,
- When associated external agencies (e.g., Information and Privacy Commissioner, National CIO Sub-Committee on Information Protection, RCMP) issue reports or identify emerging trends related to information security.

Chapter 2 - Organizing Information Security

This chapter describes the management structure needed to coordinate information security activities including who coordinates them and what agreements are required. This coordination applies to Commission employees and to external parties accessing or managing the Commission's information assets.

The Commission Information Systems & Technology (IST) Department requires the support of a network of contacts in the information security community to elicit advice, trends and to deal with other external factors.

2.1 - Internal Organization

a) Executive commitment to information security

Executive must set direction and provide support for information security by:

- Ensuring that information security reviews and audits are supported;
- Assisting business units when conducting security threat and risk assessments;
- Approving reasonable capital and operating expenses necessary to provide adequate information security for the Commission;
- Employing a dedicated information security specialist;
- Identifying and reporting significant threat changes and exposures to threats of assets associated with information security;
- Supporting the IST department in their implementation of security controls, training and awareness.

b) Information security specialist responsibilities

Planning and implementation of information security activities across the Commission must be coordinated by the Senior Network Security Analyst by:

- Interpreting the Information Security Policy to assist in the delivery of business functions;
- Evaluating information security implications of new Commission initiatives;
- Performing information system security risk analysis activities;
- Performing information security assessments and reviews;
- Evaluating new threats and vulnerabilities;
- Investigating information security incidents;
- Advising on the information security requirements for documented agreements with third party service providers;
- Identifying general business trends and emerging technologies, and recommending changes to
- Information Security staff training;
- Analyzing and providing advice on emerging information security standards; and,
- Providing information security advice for business areas.

c) Information Owners

Information Owners are Commission staff who have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure and working with the IT department will:

- Determine business requirements including information security needs;
- Ensure information and information systems are protected commensurate with their information
- classification and value;
- Define security requirements during the planning stage of any new or significantly changed
- information system;
- Determine authorization requirements for access to information and information systems;
- Approve access privileges for each user or set of users;
- Document information exchange agreements;
- Develop service level agreements for information systems under their custody or control;
- Implement processes to ensure users are aware of their security responsibilities;
- Monitor that users are fulfilling their security responsibilities; and,
- Be involved with security reviews and/or audits.

d) Confidentiality agreements

Confidentiality agreements reflecting organizational requirements for the handling of information must be in place and reviewed regularly by contract owners (contractor managers) and the Specialist of Procurement & Internal Policy.

Information Owners must:

- Ensure employees are informed of their obligation to maintain the confidentiality of information; and,
- Ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated annually.

e) Contact with service providers

Appropriate contacts shall be maintained with service providers of information technology and services including but not limited to:

- Internet service providers;
- Vendors of security and monitoring software or appliances in use at the Commission;
- Internal network service providers (including firewalls and network intrusion protection services).

f) Information Technology Department staff

Personnel with information security responsibilities must maintain their knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities by:

- Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories;
- Maintaining and improving knowledge regarding information security best practices; and,
- Creating a support network of other security specialists.

g) Approval for information systems

Information Custodians of a new or significantly modified information system must, with the assistance of the IT department:

- Conduct a Security Threat and Risk Assessment;
- Address security requirements in the development of the system;
- Conduct a risk and controls review to determine if controls are adequate to mitigate business risks prior to implementation of the information system; and,

Prior to acquisition of new hardware, firmware or software, Information Custodians must consult with the IT Department to:

- Evaluate compatibility with existing information systems hardware, firmware and software;
- Ensure new hardware, firmware and software conform to the Information Security Policy, standards and guidelines;
- Consider the reliability of the product as part of the procurement selection process; and,
- Evaluate the need for any additional security measures and the impact on existing security processes.

Personnel must not store Commission information on non-Commission hardware, off-site storage, web or cloud services unless authorized by the IT department. The IT department must test non-Commission systems for vulnerabilities prior to utilizing the hardware or service.

2.2 - External Parties

a) Risk assessment related to external parties

Assessment of risks from external party access to Commission information or information systems must be undertaken and appropriate security controls implemented.

Information Owners are responsible for assessing the business requirements and associated risks related to external party access to information and information systems.

Risk assessments must be documented during the conceptual design phase of a project and updated throughout the lifecycle of the information system (e.g., prior to and following technical or business process changes to the information system).

The assessment of risks related to external party access must consider:

- If existing controls prevent external parties from accessing facilities or information that are not needed to meet the business requirements for the access,
- Impacts to the controls of the information processing facilities involved,
- The classification of the information assets,
- Policies and processes the external party has for personnel hiring, training (on security and privacy issues) and incident reporting,
- Internal and external processes for managing and reporting security and privacy incidents,
- Processes for identifying, authorizing, authenticating and reviewing access rights of personnel and systems of the external party,
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information,
- Impacts to both parties resulting from assets being unavailable, and,
- Data integrity requirements including impacts of accessing or using inaccurate information.

Prior to authorizing access by external parties to information and information systems Information Owners must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g. services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

b) Addressing security when dealing with external parties

Identified security requirements must be addressed prior to granting external parties access to information, information systems or information processing facilities.

Prior to authorizing access by external parties to information and information systems Information Owners must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g. services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

c) Addressing security in external party agreements

Arrangements involving external party access to information, information systems or information processing facilities must be based on a formal contract containing necessary security requirements.

Information Owners must ensure access to information assets and information processing facilities by external parties is only provided after an access agreement has been completed.

Access agreements must include:

- Roles and responsibilities of the Information Owner, Information Custodian and the external party;
- Approved security controls;
- Conditions for contract termination;
- Audit and compliance monitoring rights, responsibilities and processes;
- Reporting obligations for suspected or actual security and privacy incidents;
- Renewal and extension conditions; and,
- Requirements for regular compliance reviews.

Approved forms of agreement include:

- General Service Agreement for purchase of goods or services;
- Agreements for Alternate Service Delivery or Public Private Partnership;
- Information Sharing Agreement; or,
- Other forms of agreement as approved by Legal Services.

Information Owners must ensure the security requirements of external party access agreements include:

- Notification of obligations of the parties to adhere to legislation and regulation;
- Requirements to adhere to agreed information security policies and procedures;
- Processes for amending the agreement;
- Acknowledgement by the external party that ownership of information is retained by the Commission;
- Confidentiality obligations of the external party and their personnel or agents;
- Requirements for use of unique user identifiers;
- Processes for conducting audits and compliance monitoring activities;
- Responsibilities and processes for reporting security and privacy incidents; and,
- Assurances that disciplinary action will be applied to employees or contractors who fail to comply with the terms of the agreement.

Chapter 3 - Asset Management

Information and information systems services constitute valuable Commission resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, this chapter specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

This chapter sets the foundation for a system that classifies information to identify different security levels, to specify how much protection is expected and how information should be handled at each level. Not all the information requires the same level of protection because only some information is sensitive or confidential.

3.1 - Responsibility for assets

There is a need to identify and manage information and information technology assets associated with information systems or services ("assets") to provide control and accountability, support strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

a) Identification of assets

Information Custodians must identify assets under their control including:

- Software;
- Hardware;
- Services including computer and communications services, and general utilities;
- Information assets required to be inventoried in the personal information directory (required under the Freedom of Information and Protection of Privacy Act); and,
- All other information assets including: database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.

b) Documenting and maintaining asset inventories

The Information Custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of the Commission risk management strategy.

Information Owners with the assistance of Information Custodians must document, maintain and verify information assets

The following information should be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- License information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions;
- Consequences of loss.

c) Loss, theft or misappropriation of assets.

The loss, theft or misappropriation of assets must be reported. Where the loss, theft or misappropriation involves information the Information Owner and IT Department must be immediately notified. Where the loss, theft or misappropriation involves hardware (computers, phones, portable media, etc.) the IT department must be immediately notified.

3.2 - Designating Information Owners/Custodians

Information Owners and Custodians must be designated for all assets associated with information systems.

a) Responsibilities for Information Owners

An Information Owner is responsible for controlling the production, development, maintenance, use and security of information assets within their jurisdiction. Information Owners are responsible for:

- Working with the IT Department to ensure the appropriate safeguarding of information and technology systems or services;
- Defining and regularly reviewing access restrictions and safeguards of their designated information; and,
- Bringing any information security concerns to the immediate attention of the IT Department.

b) Responsibilities of the IT Department

The IT Department is the Custodian of all information and technology systems or services within the Commission and is responsible for:

- Overseeing the functioning of information and technology assets;
- End-to-end security of information assets;
- Delivery of services in accordance with defined service requirements; and,
- Regular reporting on designated information and technology assets.

3.3 - Acceptable use of Commission resources

Rules for the acceptable use of information systems must be identified, documented and implemented to help prevent misuse or compromise of Commission information systems.

a) Acceptable use of Commission resources

All users of the Commission's information systems must take responsibility for, and accept the duty to actively protect the Commission's information and technology assets. Expectations for the use of Commission information systems are described in the *Usage of IT Resources Policy*. Compliance with the usage policy is critical in securing Commission information assets.

The requirements for personal use of Commission information systems are described in the *Usage of IT Resources Policy*.

3.4 - Information classification

The Commission does not employ a formal information security classification system. Information owners must take into account the value, sensitivity and intended use of the information when creating and reviewing access restrictions for:

- Internally shared files;
- IS systems (financial records, well records, etc);
- Files accessible by the public or third parties (FTP, websites, etc.); and,
- Email or other electronic communications.

a) Information handling/transmission procedures

Information deemed sensitive or confidential must only be transmitted via an encrypted method. These methods include:

- Encrypted USB storage provided by the IT department;
- SSL web connection with minimum TLS 1.0 and 256 bit keys;
- TLS FTPS transfer; and,
- Internal SMB file transfers.

Information deemed sensitive or confidential must also have an authentication method prior to providing access.

b) Information storage procedures

Storage of information assets has the following requirements:

- All information is stored with the assumption it is confidential;
- Portable devices and systems (including phones, laptops, USB media) must be encrypted;
- Files shares and not local laptop drives are used to store information with the exception of local email profiles and caches.
- The IT Department is responsible for all hardware related to the storage of information at the Commission.

Chapter 4 - Human Resources Security

This chapter identifies the information security requirements for personnel that have an employment relationship with the Commission. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of Commission assets, information and services.

This chapter references the terms and conditions set by the Commission for employees and identifies the conditions for external personnel such as contractors or volunteers

Management and personnel have different security responsibilities and liabilities that apply prior to, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish management responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or has changed.

4.1 - Prior to employment

a) Security roles and responsibilities

Information Owners must:

- Document information security roles and responsibilities for personnel in job descriptions, standing offers, contracts, and information use agreements; and,
- Review and update information security roles and responsibilities when conducting staffing or contracting activities.

b) Communication of security roles and responsibilities

Managers must ensure personnel are informed of their security roles and responsibilities by establishing processes for communicating security roles and responsibilities to protect information system assets.

4.2 - Personnel screening must be performed prior to employment

a) Personnel screening

Personnel should be screened to assess their: education, skills, knowledge, experience, and past work performance. The screening should also confirm the applicant's identity.

The extent of the screening process should be commensurate with the sensitivity of the information (identified by the information owners) and nature of work to be performed.

This screening applies to future staff, contractors or volunteers.

b) Criminal records screening

HROD, on the recommendation of the hiring manager, will designate positions requiring criminal records checks. The Commissioner must approve all designated positions. Positions with the following primary functions must be designated:

- Positions having access to sensitive information. Sensitive information can be about employees, clients or others and may be held by the Commission is any information that, if compromised, could result in serious consequences for individuals, organizations, or the Commission.
- Positions with expense/budget authority and/or revenue authority in excess of $500,000.
- Positions responsible for Commissions corporate safety and/or security.
- Positions responsible for and who have unrestricted access to operational, data and information management systems where the disruptions of such a system could significantly impact services or reveal confidential information.
- Senior leadership and executive positions

4.3 - During employment

a) Management responsibilities

Management must ensure personnel comply with security policies and procedures. Managers must support the implementation of information security policies and practices by:

- Ensuring personnel are informed of information security roles and responsibilities prior to being granted access to information or information systems;
- encourage staff to participate in IT department sponsored information security training;
- Ensuring personnel to adhere to information security policies and are duly informed that any breach of security rights may include discipline up to and including termination;
- Reviewing and validating security roles and responsibilities in all job descriptions, standing offers, contracts and information use agreements on an ongoing basis.

4.4 - Information security training and awareness of security policy

Personal awareness and education of security threats, risks and concerns and information security policies and procedures are required for all Commission staff to help protect the Commission against electronic threats.

a) Orientation for new personnel

The IT Department is responsible for designing, developing and delivering an information security awareness orientation processes that all personnel (regular, contract, volunteer) must complete prior to being granted access to any electronic information systems.

The IT department must ensure there is a specific/separate training module for all managers and supervisors to ensure roles and responsibilities and non-compliance consequences are clearly understood.

b) Ongoing information security awareness, education and training

The IT Department must provide at a minimum of once per year ongoing information security awareness, education and training, addressing topics including but not limited to:

- Protection of information;
- Known information security threats;
- Legal responsibilities;
- Information security policies and directives;
- Procedures for reporting information security events to the IT Department;
- Appropriate use of Commission resources;
- How to obtain security advice;
- File storage and transmission security for Information Owners; and,
- Application management (email, Service Desk, etc.).

4.5 - Security breaches and policy violations

a) Reviewing security breaches and policy violations

Upon receipt of information identifying personnel responsible for a security breach or policy violation, managers and Information Owners are responsible for:

- Ensuring the IT and HROD Departments are notified immediately of the potential security breach or policy violation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with the HR Department, if disciplinary action is warranted for employees;
- Determining if disciplinary action is warranted for non-employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

Upon receipt of information identifying personnel responsible for a security breach or policy violation, the IT Department will follow a security breach process (Information Incident Management Process).

4.6 - Termination or change of employment

a) Termination of employment

Managers must advise outgoing personnel of ongoing confidentiality responsibilities that continue to apply after termination of employment as per the Employee Code of Conduct and Ethics policy.

b) Return of assets

Managers must document the return of Commission assets in the possession of personnel upon termination of their employment. Return of assets includes:

- documents, files, data, books and manuals in physical or other media formats including other information assets developed or prepared by an employee or contractor in the course of their duties,
- computer hardware, software and equipment (e.g., mobile devices, portable media), and access devices, cards, vouchers and keys (e.g., credit cards, taxi cards, travel vouchers);
- Returned items are verified against established asset inventories;
- Recovery or compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items; and,
- Identification of unreturned access devices, cards and keys that could permit unauthorized access or alteration/destruction of assets, so that information and/or security systems can be protected.

c) Reduction of access rights

The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

Managers must review access to information systems and information processing facilities when personnel change employment, including:

- When personnel assume new roles and responsibilities;
- During restructuring of positional or organizational roles and responsibilities;
- When personnel commence long-term leave; and,
- Updating directories, documentation and systems.

Managers must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment status by contacting the IT Department, Corporate Property Department and also the IS Department if the employee had access to IS systems (Kermit, IRIS, AMS, etc). This contact should be in the form of a Service Desk employee exit at least one week prior to exit.

The IT and IS departments are responsible for removing access from files and systems by midnight of the employee exit or by the specific time mentioned by the manager if the time of day is to be earlier than midnight.

Corporate Property department is responsible for receiving all physical access keys and cards by the time the employee leaves the premises on his/her last day.

Chapter 5 - Physical and Environmental Security

This chapter identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities. One of the principles used for protection is the use of security zones to place computers and information in secure areas. Safety measures for equipment installations are also described.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of Commission information and information systems.

5.1 - Secure areas

Commission information processing facilities must be protected by a physical security perimeter to prevent unauthorized physical access.

a) Security perimeter

All information processing facilities are a Restricted Access Security Zone.

Appropriate security controls must be applied to reduce the level of identified risks and include:

- A structure that prevents external visual and audio observations and complies with all local building codes for structural stability (external walls, internal walls, ceilings and doors).
- Appropriate access control mechanisms must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring staff to take immediate action;
- Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone;
- Commission information processing facilities must be physically separated from those managed by third parties.
- Escorting visitors;
- Securing sensitive or valuable information and assets when leaving the work areas; and,
- Taking precautions when discussing sensitive information.

b) Entry controls

Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Access to any Commission information processing facility or areas where sensitive information is kept must be restricted. These rules must be followed when accessing server rooms and wiring closets:

- Only IT personnel have access to these areas;
- Visitors must be accompanied by IT personnel;
- Personnel must challenge anyone in a secure area who is not accompanied by IT personnel;
- Visitors must sign in and obtain temporary access badges from reception.
- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Access rights to secure areas must be reviewed and updated regularly.

c) Physical security requirements

Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.

The IT department must design, document and approve security controls for information processing facilities. Considerations must include:

- Determining security perimeter and maintenance factors;
- Establishing appropriate security zones;
- Design and construction complying with health and safety regulations and standards;
- Selecting unobtrusive sites and keep signage to the minimum required for meeting fire and other safety requirements;
- Limiting the identification of information processing facility locations, in publicly and internally available directories, to the minimum required; and,
- Selecting sites so that public access can be strictly controlled or avoided.

d) Other secure area requirements

- Activities within a secure area are confidential and must not be discussed in a non-secure area, or with persons who do not have a need-to-know;
- Sensitive information must not be discussed with persons without a need-to-know; and,
- Maintenance staff and cleaners need not have unescorted access to secure areas.

5.2 – Site considerations

a) Design and site selection

Physical security controls must be designed to protect against damage from natural or man-made disaster.

The IT Department and site planners (Corporate Property Administration) must incorporate physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to meeting building code specifications and fire regulations:

- Combustible or hazardous materials must be stored at a safe distance from the secure area. Bulk supplies must not be stored within the secure area;
- Installing camera monitoring systems;
- Installing fire alarm and fire suppression systems;
- Installing humidity sensors and alarms;
- Installing temperature sensors and alarms;
- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements; and,
- Fallback equipment (e.g., for DRP) and backup media must be sited at a safe distance to avoid damage from a disaster affecting the main site.

b) Equipment location

The IT department is responsible for ensuring that the design and layout of information processing facilities provides protection from security threats. Safeguards must include:

- Locating servers and other centralized computing equipment within a Restricted Access Security Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas;
- Ensuring that kiosks and public terminal safeguards are in place.

c) Equipment protection

The IT department is responsible for ensuring that the design and layout of information processing facilities provides protection from physical and environmental hazards. Safeguards must include:

- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Ban eating and drinking in work areas containing equipment (other than personal computers);
- Briefing personnel who work with equipment about safety practices in the workplace;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems;
- Equipment, information or software belonging to the Commission must not be removed from premises without prior authorization; and,
- Regularly inspecting the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

d) Off-site equipment security controls

Equipment must be protected when off-site from Commission sites to guard equipment from loss or unauthorized access.

The IT Department must ensure that Commission equipment being used off-site is protected, matching with the sensitivity of the information it contains and the value of the equipment. These controls must be in place:

- Portable computers are encrypted;
- Equipment is protected from unauthorized access by the use of a password;
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate;
- Personnel are familiar with operation of the protection technologies in use;
- Not leave Commission equipment unattended in a public place;

- Ensure that equipment is under their direct control at all times when travelling;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately to the IT Department.

5.3 – Disposal or re-use of storage devices

a) Erasure or reassignment of hardware and media

Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed.

The IT Department must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned within the Commission, forensically wiped or destroyed.

Prior to reassignment of hardware or media within the Commission it must be ensured that:

- That the integrity of Commission records is maintained by adhering to Records Management policies;
- Information and software is erased using methods and standards approved by the Office of the Government Chief Information Officer; and,
- Asset inventories are updated to record details of the erasure and reassignment including:
    - Asset identifier,
    - Date of erasure or reassignment; and,
    - Names of personnel conducting the erasure or reassignment.

b) Destruction of hardware

The IT Department is responsible for ensuring hardware media used to store information or software is destroyed in a secure manner if forensic erasure is not possible.

Chapter 6 – Information Security Services

This chapter establishes a framework to support the integration of information security in the services provided by the Commission information processing facilities.

Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve.

Controls for operations include documented processes, staff duties and formal methods to implement systems and changes. This includes:

- Methods to protect information;
- Create copies for back-up and to manage the retention schedules; and,
- Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

6.1 – Security Documentation

a) Operations documentation

Operations documentation must contain detailed instructions regarding:

- Information processing and handling;
- System re-start and recovery;
- System testing after maintenance;
- Back-up and recovery, including on-site and off-site storage;
- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Server room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and,
- Operations, technical, emergency and business contacts.

b) Information Risk

Information Owners with the assistance of the Information Custodians must document the risks associated with the information they control through these methods:

- Identifying the sensitivity and confidentiality of information;
- Assessing the potential business impact, including the security impact, of information loss or theft;
- Identifying information retention periods;
- Identifying test procedures for secure access to data to assist with checks after maintenance and changes;
- Assessing any information access monitoring requirements for sensitive data; and,
- Assessing current data backup and server snapshot schedules.

6.2 – Change Management

a) Planning changes

Information Custodians must plan for changes by:

- Assessing the impact of the proposed changes on security;
- Identifying impacts to dependant services;
- Identifying the impact on agreements with business partners and third parties including information sharing agreements, Memoranda of Understanding, licensing and provision of services;
- Preparing change implementation plans that include testing and contingency plans in the event of problems;
- Obtaining approvals from affected Information Owners;
- Notifying in advance all affected parties; and,
- Training technical staff and operations staff if required.

b) Implementing changes

Information Custodians must implement changes by:

- Notifying affected parties, including business partners and third parties;
- Minimizing impact to business parties or staff;
- Training users if required;
- Documenting and reviewing the documentation throughout the testing and implementation phases;
- Recording all pertinent details regarding the changes; and,
- Checking after the change has been performed that only the intended changes took place.

6.3 - Segregation of duties and systems

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems.

a) Segregation of duties

Information Owners and Information Custodians must reduce the risk of disruption of information systems by:

- Requiring complete and accurate documentation for every information system;
- Rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on key systems;
- Automating functions to reduce the reliance on human intervention for information systems;
- Requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- Maintaining a role based access password database organized such that no single individual has sole access to a system;
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action; and,
- Implementing information systems security controls to minimize opportunities for collusion.

b) Separation requirements for systems

The goal is to reduce the risk of unauthorized or inadvertent changes to operational information systems or information systems under development or being tested. Development and test information systems must be separated from operational information systems.

Information Custodians must protect operational information systems by:

- Separating operational environments from test and development environments using different servers (virtual or physical), storage partitions and networks if required;
- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified personnel;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;
- Limiting the use of personal information in development, test or training information systems.

6.4 – External Services

a) External service delivery management

Prior to using external information and technology services - security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.

Information Owners and Information Custodians must include security requirements in procurement documents for information and information system services being delivered by external parties. Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and,
- Developing transition and fall back plans (e.g., migration from one service provider to another).

b) Service level continuity

Information Custodians must ensure service agreements with external parties document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process owners;
- Audit and compliance monitoring rights and responsibilities;
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained; and,
- Reviewing the adequacy of the service provider's contingency plans for responding to disasters or major service failures.

Commission personnel managing external service delivery must regularly monitor and review services, reports and records provided by external parties and carry out regular audits.

c) Monitoring and review of external party services

The Commission must regularly monitor and review services, reports and records provided by external parties and carry out regular audits to ensure compliance with security policies.

Information Custodians must establish processes to manage and review the information security of external party delivered services by:

- Assigning responsibility for monitoring to a designated staff member;
- Ensuring audit provisions are included in service delivery contracts;
- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
    - Conducting internal self-assessments of control processes,
    - Requiring external parties to submit annual management assertions that controls are being adhered to,
    - Conducting independent security reviews, audits and updates to risk and controls reviews, and,
    - Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents.
- Establishing performance measures to ensure adequate service levels are maintained and measured.

d) Change management processes for external party services

Change management must provide assurance that changes to information system services delivered by external parties maintain or enhance security controls.

Information Custodians must ensure agreements with external party service providers include provisions for:

- Amending agreements when required by changes to legislation, regulation, business requirements, policy or service delivery; and,
- Requiring the service provider to obtain pre-approval for significant changes involving:
    - Network services,
    - New technologies,
    - Use of new or enhanced system components (e.g., software or hardware),
    - System development, test tools and facilities,
    - Modification or relocation of the physical facilities, and,
    - Sub-contracted services.

Information Custodians must ensure the change management process for information systems services delivered by external parties includes, as required:

- Reviewing and updating the Security Threat and Risk Assessment to determine impacts on security controls;
- Implementing new or enhanced security controls where identified by the risk assessment;
- Initiating and implementing revisions to policies and procedures; and,
- Revising personnel awareness and training programs.

6.5 - System planning and acceptance

The use of information system resources must be monitored, optimized and projections made of future capacity requirements to reduce the risk of system failures and unacceptable performance levels.

a) Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes,
- Including capacity requirements in service agreements;
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
    - New business and information systems requirements,
    - Statistical or historical capacity requirement information, and,
    - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

b) Resource capacity planning

Information Custodians must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a threat to system security or services.

c) System acceptance process

Information Owners must ensure that system acceptance criteria are defined as part of the system development and acquisition process to ensure that new or upgraded information systems are tested against defined, agreed and documented criteria for acceptance, prior to becoming operational.

Prior to implementing new or upgraded information systems, Information Custodians must ensure:

- System acceptance criteria are identified including privacy, security and systems development; and,
- Security controls are accepted by the Senior Network Security Analyst.

d) System acceptance criteria

Information Custodians must document system acceptance criteria, including:

- Projected performance and resource capacity requirements;
- Disaster recovery, restart, and contingency plans and procedures;
- Impact on standardized routine operating procedures and manual procedures;
- Implementation of security controls;
- Assurance that installation of the new system will not adversely affect existing systems, particularly at peak processing times;
- Disaster Recovery arrangements;
- Training requirements; and,
- User acceptance testing.

e) Security certification

Information Custodians must receive assurance that a new or updated information system meets minimum security acceptance criteria.

Assurance should be obtained from the Senior Network Security Analyst who will conduct a security controls review which determines whether a system includes adequate controls to mitigate security risks. This process will also determine the effect of the new system on the overall security of Commission information systems.

f) System accreditation

Information Custodians must authorize the implementation of new or upgraded information systems based on the degree to which the acceptance criteria are satisfied.

6.6 - Protection against malicious and mobile code

Security awareness, prevention and detection controls must be utilized to protect information systems against malicious code.

a) Prevention and detection controls

Information Custodians must protect Commission information systems from malicious code (e.g., viruses, worms) by undertaking such activities as:

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malicious code before use; and,
- Maintaining business continuity plans to recover from malicious code incidents.

The Senior Network Security Analyst must ensure processes are implemented to:

- Maintain a critical incident management plan to identify and respond to malicious code incidents; and,
- Maintain a register of specific malicious code countermeasures (e.g., blocked websites, blocked electronic mail attachment file types and blocked network ports) including a description, the rationale, the approval authority and the date applied.

b) Active controls

The Senior Network Security Analyst must ensure there are more proactive measures in place. These include:

- Intrusion detection system on the edge of network;
- Scanning for code exploits on servers and systems; and,
- Email pre-scanning that goes beyond malicious code definitions and scanning heuristics.

c) User awareness

The Senior Network Security Analyst is responsible for developing a user awareness program which will include education on malicious code countermeasures.

The Senior Network Security Analyst is responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

Mobile code must be restricted to the intended information system or environment. a) Mobile code categorization

d) Restrictions on mobile code

Mobile code must be restricted to the intended information system or environment.

To protect information systems from malicious mobile code these rules must be followed:

- Obtain digitally signed mobile code from trusted sources;
- Method implemented for blocking receipt or execution of mobile code;
- Use configuration controls to resist known exploits; and,
- Users should not access websites where the certificate is invalid.

6.7 - Back-up

Information and information systems must be backed up and the recovery process tested regularly to enable the timely recovery of information and information systems.

a) Defining requirements

Information Custodians with input from Information Owners must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
  - Business continuity plans,
  - Policy, legislative, regulatory and other legal obligations, and,
  - Records management requirements, including the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS); and,
- Documenting the backup and recovery processes including:
  - Types of information to be backed up,
  - Schedules for the backup of information and information systems,
  - Backup storage management (e.g., retention period, pattern of backup cycles),
  - Methods for performing, validating and labelling backups, and,
  - Methods for validating recovery of the information and information system.

b) Safeguarding backup facilities and storage

Information Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards may include:

- Using encryption to protect the backed up information;
- Using digital signatures to protect the integrity of the information;
- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup data at a sufficient distance to escape any damage from a disaster at the main site.

c) Testing

Information Custodians must regularly test backup and recovery processes.

6.8 - Network security management

A range of controls must be implemented to achieve and maintain security within the Commission network.

a) Control and management of networks

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems. The Senior Network Security Analyst is responsible for approving the design and implementation of these systems and controls.

Selection of controls must be based on a Security Threat and Risk Assessment, taking into account the information security classification determined by the Information Owners, and applicability to the network technology.

The Security Threat and Risk Assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and cryptographic keys;
- Network management information;
- Network pathways and routes;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and,
- Information system interfaces to networks.

b) Configuration control

To maintain the integrity of networks, Information Custodians must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;
- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

c) Secured path

Where required by information classification, information must only be transmitted using a secured path.

Secured paths for information transmission must use controls such as data or session encryption, such as SSH, SSL or VPN tunnels.

d) Wireless Local Area Networking

Wireless Local Area Networks must utilize the controls and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by the IT Department;
- The use of strong, frequently changed, encryption keys and passwords or central authentication method like Radius;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Where supported by information classification, additional controls for wireless networks may include:

- Virtual Private Network tunnel technology;
- The use of Desktop Terminal Services (DTS) technology; and,
- Intrusion detection systems, firewalls and Media Access Control (MAC) address filtering.

e) Equipment management

Information Custodians must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

f) Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

- Traffic traversing network security boundaries;
- Traffic within networks housing sensitive or mission critical systems or information;
- Security-relevant events on network devices, such as operator login and configuration changes; and,
- Security-relevant events on systems that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g., automation of log monitoring and event alerting).

Active automated surveillance of networks must be implemented to detect and report on security events (e.g., network intrusion detection systems).

g) Coordination and consistency of control implementation

Information Custodians must document network security controls in the System Security Plan including:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures (including monitoring frequency, review and remediation processes).

h) Network service agreement

Security features, service levels and management requirements of all network services must be documented and included in any network service agreement.

Formal network service agreements must be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services.

The network service agreement must include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and,
- The requirement to meet or exceed Commission security policy and standards.

Information Custodians must confirm that the specified security features are implemented prior to commencement of service delivery.

6.9 - Media handling

All removable computer media must be managed with controls appropriate for confidential or sensitive data. Treating all data classifications the same will reduce human error

a) Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

All portable storage devices must have whole disk encryption enabled by the IT Department before personnel can store Commission data on them. Only the IT Department can approve the type and make of a portable storage device.

Whenever possible, other data transmission methods should be used before information is stored on portable storage devices.

b) Human factors

Information Custodians and Managers must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with the encryption requirements;
- Familiar with operation of the required protection technologies and when they must not be used; and,
- Familiar with security event and loss reporting procedures.

c) Risk assessment factors

The Security Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media destruction;
- Improper long term storage environment;
- Exposure to malicious and mobile code; and,
- Incomplete erasure of data prior to device disposal.

Information classification and sensitivity levels must be considered in the risk assessment.

d) Mandatory controls

Minimum information protection safeguards for the use of portable storage devices include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Treating all Commission data on portable storage devices as sensitive;
- Not storing the only version of a document on portable storage devices;

- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices;
- Prevention of mobile and malicious software,
- Logging of media custody and location to allow for:
    - Accounting and audit,
    - Media labelling to indicate owner,
    - Maintenance of information where the information storage requirement exceeds the expected media lifetime, and,
    - Secure erasure and disposal.

e) Secure disposal of media

Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

Information Custodians must ensure that media that is no longer required operationally (e.g., due to expiry, surplus, damage or wear), is disposed of securely.

Media disposal procedures must:

- Be documented and communicated to personnel;
- Specify erasure and disposal measures whose strength is based on information sensitivity and type of media (e.g., erasure software);
- Include secure destruction of media if erasure is not sufficient, or not cost effective (e.g., destruction by shredding, incineration or chemical dissolution);
- Include secure storage measures for media collected for and awaiting erasure or disposal, to avoid undetected theft of small amounts of media from large volumes awaiting disposal; and,
- Include audit logs of media disposal.

f) Media handling procedures

Media must be handled and stored so as to prevent unauthorized information disclosure or misuse.

All removable computer media must be handled with controls appropriate for confidential or sensitive data.

The IT Department is responsible for media handling documentation which must include procedures for:

- Access control restrictions and authorization;
- Correct use of technology (e.g., encryption) to enforce access control;
- Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
- Operating the media storage environment and managing media lifespan according to manufacturer specifications;
- Regular status accounting of media;

- Maintenance of media transfer and storage records;
- Media destruction and disposal;
- User training; and,
- Use of non-Commission storage devices.

g) Protection of systems documentation

Information Custodians must ensure that documented procedures for the secure use and storage of systems documentation are established and followed. Procedures must:

- Require information classification labelling of system documentation;
- Establish lists of users authorized to access system documentation on a 'need to know' basis;
- Establish handling rules for the information regardless of storage media (e.g., electronic, paper);
- Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification; and,
- Include a compliance monitoring process.

h) Electronic information exchange

The Senior Network Security Analyst must document and implement procedures to protect information from interception, copying, misrouting and destruction when being transmitted electronically or verbally. Transmission methods include but are not limited to:

- E-mail, including attachments;
- Electronic file transfer (e.g., File Transfer Protocol (FTP), HTTPS transfers);
- Use of mobile devices;
- Telephone, cell, and other voice messaging;
- Faxes; and,
- Instant messaging.

6.10 – Exchanges of information

Information and software exchange agreements between the Commission and other organizations (including government) must be documented.

a) Exchange agreements

Information Custodians must ensure the terms and conditions for exchanging information assets with external parties is documented in an agreement. The agreement must define:

- Custody and control accountabilities;
- Authority of a custodian to publish, grant access to or redistribute the information;
- Purpose and authorized uses of the information or software;
- Limitations on data linkage;
- Duration, renewal and termination provisions;
- Primary contacts, for agreement, governance and management;

- Requirements for:
  - Protecting information according to its security classification,
  - Handling information (e.g., recording authorised recipients, confirming receipt of transmitted data, periodically reviewing records of authorised recipients),
  - Labelling information (e.g., methods to be used to apply and recognize labelling),
  - Maintaining integrity and non-repudiation of information, and,
  - Media management and destruction;
- Technical standards for transmission, recording or reading information or software;
- Responsibilities for reporting privacy and security incidents and breaches;
- Liability, accountability and mitigation strategies, for attempted, suspected or actual privacy and security incidents and breaches; and,
- Problem resolution and escalation processes.

b) Information and software exchange requirements

Information Custodians must ensure the following are completed for the information or software covered by the exchange agreement:

- An approved Privacy Impact Assessment; and,
- A Security Threat and Risk Assessment.

Exchange agreements must be reviewed by legal counsel for the Province prior to being signed.

c) Media transport procedures

Media being physically transported must be appropriately protected to protect information from unauthorized disclosure or loss.

Minimum media transport requirements are:

- Using couriers that are approved by government;
- Inspecting identification credentials of couriers upon pickup and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage;
- Packaging so that the sensitivity of the media is not displayed and the package is discreet; and,
- Using notifications of transport activities, such as:
  - Sender informing receiver of the impending shipment, and,
  - Receiver confirming receipt of the shipment;

Information transmitted by electronic messaging must be appropriately protected. a) General requirements

d) Electronic messaging services

Information transmitted by electronic messaging must be appropriately protected.

Electronic messaging services must be managed to protect the integrity of Commission messages by:

- Protecting messages from unauthorized access, modification or denial of service;
- Ensuring correct addressing and transportation of messages;

- Providing reliable and available messaging infrastructure; and,
- Conforming to legislative, regulatory and policy requirements.

The Senior Network Security Analyst must approve implementation of, and significant modification to, electronic messaging systems.

Personnel must support the responsible use of electronic messaging services by:

- Using only Commission electronic messaging systems;
- Using only authorized encryption for e-mail or attachments; and
- Not automatically forwarding Commission e-mail to external e-mail addresses;

Electronic messages created, compiled on, sent or received on Commission information systems are records of the Commission. These records:

- Are the property of the Government of British Columbia;
- Must be managed in accordance with the Document Disposal Act and the policies, standards and procedures in the Recorded Information Management Manual; and,
- Are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

e) Information in business information systems

Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.

Information Custodians must document and implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support the Commission such as e-mail, calendars and financial systems. The same standards apply to business and industry information held by the Commission.

A Security Threat and Risk Assessment must be conducted to:

- Determine if business information systems provide sufficient protection for the information being shared;
- Define controls to manage information sharing;
- Reduce the risk of social engineering; and,
- Identify access control requirements.

6.11 - Electronic commerce services

Information in electronic commerce information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.

a) Electronic commerce

Prior to initiating or implementing electronic commerce information systems Information Custodians must:

- Ensure that the Security Threat and Risk Assessment is conducted and addresses threats and risks related to electronic commerce;
- Confirm that a Privacy Impact Assessment has been conducted and approved;
- Determine the security classification of the information and information system(s) involved;

- Ensure that the user notification and acceptance of terms and conditions of use complies with Commission policies and standards;
- Ensure multi factor authentication is used commensurate with the sensitivity and value of the information;
- Develop and implement processes to maintain content currency;
- Confirm the information system has received security certification and accreditation; and,
- Develop Disaster Recovery Plans.

b) On-line transaction security

To maintain the confidentiality, integrity and availability of on-line transactions in information systems, Information Custodians are responsible for ensuring information systems containing on-line transactions implement security controls commensurate with the value and sensitivity of the information.

Security controls must be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

c) Payment card transaction security

Information Custodians are responsible for ensuring that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry Data Security Standard.

The Payment Card Industry Data Security Standard V2.0 has 12 high-level requirements:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;
- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;
- Use and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need to know;
- Assign unique ID to each person with computer access;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and,
- Maintain a policy that addresses information security for all personnel.

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

d) Security of publicly available information

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

Information Owners must approve the publication, modification or removal of information on publicly available information systems. Information Owners are responsible for maintaining the accuracy and integrity of the published information.

Information Custodians are responsible for developing, documenting and implementing Security controls to:

- Maintain the integrity of published information;
- Prevent the inappropriate release of sensitive or personal information;
- Monitor for unauthorized changes; and,
- Prevent unauthorized access to networks and information systems.

6.12 - Monitoring

Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.

a) Audit logging

Information Custodians must ensure that audit logs are used to record user and system activities, exceptions and information security and operational events including information about activity on networks, applications and systems. Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs. Audit logs should include, when relevant, the following information:

- User identifier;
- Dates, times and details of key events (e.g., logon and logoff);
- Logon method, location, terminal identity (if possible), network address;
- Records of successful and unsuccessful system access attempts;
- Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and type of access (e.g., view, read, modify, delete);
- Network addresses and protocols;
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems (e.g., anti-virus, intrusion detection).

Audit logs may contain confidential data and access must be restricted to personnel with 'need-to-know' privileged access and be protected accordingly.

Information Custodians should not have the ability to modify, erase or de-activate logs of their own activities. There may be cases where IT staff responsibilities overlap to an extent this is not possible.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log.

b) Audit log retention

Audit logs must be:

- Retained according to the approved retention schedule for the system or information asset; and,
- Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

c) Response to alarms

Information Custodians must establish and document alarm response procedures to ensure alarms are responded to immediately and consistently.

Under extreme threat situations, Information Custodians should have documented authority to shut down all or part of a system or network when the alarm indicates severe unacceptable threats are present. When exercising this authority Information Custodians must report the circumstances to management and Information Owners as soon as possible.

Normally, the response to an alarm will include:

- Identification of the alarm event;
- Isolation of the event including affected assets;
- Identification and isolation or neutralization of the source;
- Corrective action;
- Forensic analysis of event;
- Action to prevent recurrence; and,
- Securing of audit logs as evidence.

Some alarms indicating a system or network intrusion will require that the affected system or network not be shut down or removed from the network until a forensic analysis has taken place. This special measure is taken to avoid unintentionally notifying an attacker they have been discovered.

d) Monitoring the use of information systems

The use of information systems must be monitored and the result of the monitoring activities must be regularly reviewed.

Information Custodians must ensure that the use of information systems can be monitored to detect activities including: authorized and unauthorized accesses, system alerts and failures. Information Owners and Information Custodians must identify the activities to be reported. Information custodians must implement, manage and monitor logging systems for:

- Authorized access, including:
  - User identifier,
  - Date and time of log on and log off,
  - Type of event(s),
  - Files accessed, and,
  - Programs, privileges and/or utilities used;
- Privileged operations, including:
  - Use of privileged accounts (e.g., System Administrator, Data Base Administrator)
  - System start-up and shutdown, and,

    - Input/Output device attachment and/or detachment;
- Unauthorized access attempts, including:
    - Failed or rejected user actions, data access or other resource attempts,
    - Access policy violations and notifications for network gateways and firewalls, and,
    - Alerts from intrusion detection systems;
- System alerts or failures, including:
    - Console alerts or messages,
    - System log exceptions,
    - Network management alarms, and,
    - Access control system alarms; and,
    - Changes to, or attempts to change, system security settings and controls.

e) Review of monitoring activities

Information Custodians must set up and document processes for the review of audit logs based on the Information Owners assessment of the value and sensitivity of the information assets, the criticality of the system and the resources required for review.

Audit log reviews should:

- Prioritize reviews of high value and highly sensitive information assets,
- Be based on a documented security threat and risk assessment,
- Utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity) and facilitate ongoing analysis and review.
- Monitoring should be tested at least annually to ensure that desired events are detected. Analysis of monitoring activities can indicate:
- The efficacy of user awareness and training and indicate new training requirements;
- Vulnerabilities that could be, or that are being, exploited; or
- Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

f) Privileged activities logged

Privileged users typically have extensive system permissions not granted to most users. Information Custodians must ensure that the activities of privileged users are regularly reviewed including logging:

- Event occurrence times;
- Event details, such as files accessed, modified or deleted, errors and corrective action;
- Identity of the account and the privileged user involved; and,
- The system processes involved.

g) Reporting and logging faults

Information Custodians must implement processes for monitoring, reporting, logging, analyzing and correcting system faults reported by users and automated detection systems.

Fault logging requirements should be determined through a security threat and risk assessment. Fault management reporting should include:

- Description of fault including date/time, location, extent of fault;
- Analysis of probable source/cause;
- Actions taken to respond to and/or resolve the fault; and,
- Corrective action taken.

h) Synchronization

Computer clocks shall be synchronized for accurate reporting.

System administrators must synchronize information system clocks to:

- The local default switch gateway, domain controller; or,
- Federal government approved clock host.

Chapter 7 - Access Control

This chapter identifies the mechanisms that restrict access to Commission information and information assets. Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information (e.g., personal, sensitive or industry confidential) and by business requirements.

Access control policies provide the blueprint for the management of user access, authorizations and control mechanisms for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and personnel.

7.1 - Business requirement for access control

a) Access control policy

Access to information systems and services must be consistent with business needs and be based on security requirements. An access control policy for each information system must be created.

Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements;
- Be based upon Security Threat and Risk Assessments; and,
- Include classification of assets.
- Consider both physical and logical access to assets;
- Apply the "need to know" and "least privilege" principles;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable; and,
- Have permissions assigned to roles rather than individual user identifiers when possible.

The access control policy must be communicated to personnel as part of awareness training.

b) Access control policy management

Information Custodians are responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all personnel;
- Documenting processes for user registration and deregistration;
- Segregating roles and functions (i.e. access requests, access authorization, access administration);
- Defining rules for controlling access to privileged system functions;
- Identifying roles and/or functions which require multi factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced personnel security screening for sensitive assets.

c) Review of access control policy

Information Custodians must conduct periodic reviews of the access control policy as part of an ongoing process for risk management, security, and privacy. Reviews must be conducted:

- Annually at a minimum;
- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise; and,
- Following significant Commission staff re-organization as appropriate.

7.2 - User access management

There must be a formal user registration and de-registration process for granting access to all information systems to ensure that all access actions are traceable to an identifiable individual or process.

a) Registration

Information Custodians are responsible for managing access to the assets under their control and must implement registration processes which:

- Requires custodians to approve all access rights. This process should:
  - Ensure access requests are approved by the supervisor/manager of the user requesting access, and,
  - Ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right approvals;
- Ensures personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensures accesses are traceable to an identifiable individual or process;
- Ensures each user is assigned a single unique identifier for accessing information systems except when:
  - Required to meet limitations of technology; or,
  - Required to meet unique business requirements provided the rationale is documented and approved by the Information Custodian as appropriate.
- Restricts access by using predefined role permissions where possible; and,
- Provides secure and separate transmission of the user identifier and password to the user; and,

b) Deregistration

Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization by midnight of the employee's last day;
- Promptly review access rights whenever a user changes duties and responsibilities;
- Promptly review access rights whenever the user's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended absence or temporary assignments within 10 working days of the change of status;

- Remove access privileges for employees terminated for cause concurrent with notification to individual; and,
- Quarterly check for and remove inactive or redundant user identifiers.

c) Security Screening

The allocation and use of system privileges must be restricted and controlled to prevent unauthorized access to multi-user information systems.

Information Custodians are responsible for authorizing system privileges and must:

- Identify and document the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access to system privileges includes management or information owner approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from users concurrent with changes in job status (e.g., transfer, promotion, termination);
- Limit access to the fewest number of users needed to operate or maintain the system or service;
- Ensure the access rights granted are limited to and consistent with the users' job function and responsibilities;
- Maintain a record of users granted access to system privileges;
- Ensure use of system privileges is recorded in audit logs;
- Implement processes for ongoing compliance checking of the use of system privileges; and,
- Implement processes for regular review of authorizations in place to confirm that access is still needed and that the least number of users needed have access.

User identifiers with system privileges must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

The design of information systems should include processes for performing regular maintenance activities which avoid the requirement of system privileges.

System acquisition and development should encourage use of programs which minimize the need for users to operate with system privileges.

Privileged users should:

- Not read the data of an information asset unless authorized; and,
- Be permitted to view, but not alter, user activity logs as part of security safeguards.

d) Managing the issuance of passwords

The Commission must formally designate individuals who have the authority to issue and reset passwords. The following applies:

- Passwords shall only be issued to users whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords must transmit new or reset passwords to the user in a secure manner (e.g., using encryption, using a secondary channel, phone call);
- Whenever technically possible temporary passwords must be unique to each individual and must not be easily guessable;
- Passwords must never be stored in an unprotected form; and,

- Default passwords provided by technology vendors must be changed to a security hardened password compliant during the installation of the technology (hardware or software).

e) Access rights review

Information Custodians must formally review user access rights at regular intervals. Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When a user's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a user's need to access information assets;
- As part of a major reorganization, or the introduction of new technology or applications; and,
- When Information Custodians change the access control policy the access rights must be reviewed.

Review of access rights must include the following:

- Confirmation that access rights are based on the "need to know" and "least privilege" principles;
- Confirmation that all members of the group/role have a need to know;
- Reviews and verification of access control lists are dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights are logged and auditable.

7.3 - User responsibilities

Users must follow good security practices in the selection and use of passwords.

a) Selection of passwords

The effectiveness of access control measures is strengthened when users adopt good security practices for selecting passwords. When selecting passwords users must:

- Select complex passwords;
- Avoid using the user name or any proper names of the user;
- Avoid patterns that look complex, but are not; and,
- Avoid using the same password for multiple accounts;

A complex password is defined as being at least 12 characters long and containing at least one numeral (e.g., 1-9,0) or non-alphanumeric keyboard symbols (e.g., ! $ # %).

For mobile devices connecting to the Commission messaging server, the following password rules apply:

Passwords must contain a minimum of 4 characters if the device is set to wipe after 10 failed login attempts or 6 characters if no wiping is configured;

b) Password change

Passwords must be changed:

- During installation of computer hardware and or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected; and,
- Comply with password change instructions issued by an automated process (e.g., password lifecycle replacement) or an appropriate authority.

A user must not re-use old passwords when selecting a new password.

Privileged accounts have wider and more powerful access rights to information assets. Users authorized to create or who hold privileged accounts must use passwords which are at least 15 characters where technically feasible.

c) Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container as the token;
- Keeping a file of passwords on any computer system, including mobile devices unless that file is encrypted with a process approved by the Senior Network Security Analyst;
- Employing any automatic or scripted logon processes for personal identifiers; and,
- Using personal identifiers, access codes, or passwords associated with Commission accounts for non-Commission purposes.
- Divulging your password to anyone. Legitimate IT technical support staff such as systems administrators, helpdesk and security will not ask users for their passwords.

d) Protection of unattended equipment

Users must help prevent unauthorized access to information systems by securing unattended equipment, by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling a password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including portable storage devices; and,
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

Commission workstations and other devices used for information system access must automatically activate screen savers or equivalent locking systems after 15 minutes of inactivity or less.

e) Securing the work space

Users should secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.

- Securing the work space includes:
- Clearing desk tops and work areas;
- Securing documents and portable storage devices in a locked desk or file cabinet;
- Ensure outgoing and incoming mail is appropriately secured;
- Restarting workstations at the end of each work day;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

f) Secure work habits

Users must develop and implement security conscious work habits to reduce the likelihood of unauthorized viewing, access or disclosure of sensitive information. Security conscious work habits include:

- Ensuring sensitive information is protected from accidental viewing by persons passing through the work space;
- Ensuring that only the documents required for current work are out of their normal file cabinet;
- Covering up, filing or storing paper documents when visitors are present in the work area;
- Clearing, changing or turning off the computer screen (e.g., minimize open Windows, lock the PC) so that sensitive information is not displayed when visitors are present in the work area; and,
- Not discussing sensitive information in open work spaces or public areas.

7.4 - Network access control

Users must only be provided access to the information systems they have been specifically authorized to use.

a) Access to network services

Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

b) Management controls and processes

Information Custodians must document processes for management of network access, including:

- Documentation and review of implemented network access controls;
- Identification of threats, risks and mitigation factors associated with network services;
- Testing of network access controls to verify correct implementation; and,
- Assisting Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

c) Remote access to Commission networks or services

Providers of remote network access services for individuals must:

- Perform a Security Threat and Risk Assessment for each remote access service to determine the authentication methods to be implemented. Factors to be considered include classification of network services, information and information systems accessible from the remote access service;
- Require remote users to connect through Commission designated remote access services or security gateways (e.g., Virtual Private Network, Outlook Web Access); and,
- Require user identification and authorization prior to permitting each remote network connection.

7.5 - Network security management

Physical and logical access to diagnostic ports must be securely controlled to prevent unauthorized use of maintenance or diagnostic facilities.

a) Protection of diagnostic ports and services

To prevent bypassing of information system access controls, Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Diagnostic services like must be kept inactive until needed, and kept active for the minimum time required. (e.g. VMware SSH)

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use.

b) Segregation based on risk and requirements

Groups of information services, users and information systems must be segregated on networks and/or servers to isolate information systems, users and networks based on risk and business connectivity requirements to control information flow, minimize unauthorized connection attempts and limit the spread of damage in case of compromise.

Information Custodians must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of least privilege, management of risk and segregation of duties.

Information Custodians must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways, application layer 7 firewalls and reverse proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

The techniques and technologies selected for network segregation must be based on Security Threat and Risk Assessment findings. Factors to consider include:

- The information and information system security classification;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);
- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

Network zones should be defined and network perimeters established, according to business requirements and risk as identified in the Security Threat and Risk Assessment. For example, network zones for Public access, core network, wireless network, information system operational management and business applications could be defined, separated by network flow control points.

c) Logical and physical network connection control

Information Custodians must restrict the ability of users to physically and logically connect to networks according to the specific access control policy. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by user workstations.

d) Wireless networks

Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a Security Threat and Risk Assessment.

7.6 – Operating System Access Control

a) Information displayed before logon

Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access. This includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Displaying a general warning notice that the Information System be accessed only by authorized users;

- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

Default web pages or system management interfaces must not display information about the system that could aid an attacker.

b) Unsuccessful logon attempts

Information Custodians must configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure. If exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

A best attempt must be made to follow these rules with the exception being that not are systems are compatible with these rules.

c) Password transmission

Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

d) Allocation of unique identifier

Information Custodians must ensure users are issued unique user identifiers for their use. The process for allocating and managing unique identifiers must include:

- A single point of contact to:
  - Manage the assignment and issuance of user identifiers,
  - Ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
  - Record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

e) Shared user identifiers

In exceptional circumstances, where there is a clear business benefit identified by the Information Custodian, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and,
- The Senior Network Security Analyst approves the positional user identifier.

f) Enforcing quality password rules

A password management system must be in place for Information Custodians to provide an effective, interactive storage method that ensures quality passwords.

Information Custodians must ensure password management systems:

- Enforce the use of individual user identifiers and passwords;
- Support user selection and change of passwords using the complex password standard defined in 7.3(a);
- Enforce user change of temporary passwords at first logon and after password reset by an Administrator;
- Enforce regular user password changes every 3 months, including advance warning of impending expiry;
- Prevent re-use of passwords for a period of one year;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

Exceptions are allowed only where system limitations do not allow the enforcement of these rules. Any exceptions must be approved by the Senior Network Security Analyst.

g) Restriction and control of system utility programs

Use of system utility programs which may be used to override system and application controls must be restricted.

Information Custodians must limit use of system utility programs by limiting the ability to run such programs to privileged users. Beyond IT administrators, system privileges should only be granted to direct administrators of that specific system.

h) Session time-out

Information Custodians must implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity. Some systems may also require a connection duration limit (e.g.; VPN sessions).

Commission information systems must have session time-outs managed by operating system access, application or network infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity corresponding with the:

- Sensitivity of the system found in the Security Threat and Risk Assessment;
- Classification of the information being handled; and,
- Risks related to the use of the equipment by too many concurrent users.

The actual timeout value will vary between systems. Some guidelines are:

- Maximum timeout of 15 minutes for systems deemed the highest risk or value; and,
- Maximum timeout of 12 hours for low security systems (e.g.; VPN sessions).

7.7 - Information and application access controls

Access to information systems functions and information must be restricted in accordance with the corresponding access control policy.

a) Information access controls

Information Custodians are responsible for ensuring the implementation of the access control policies for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

- The information to be controlled;
- The system functions to be controlled; and,
- The roles authorized to access the resources/information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

b) System configuration

Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy.

c) Segregation of information

Information that is publicly accessible (non-confidential) must be segregated from non-public information. The segregation can be physical or use logical methods or controls (e.g.; file folders/shares, databases, tables, ACL's).

Information Custodians must conduct a Security Threat and Risk Assessment to determine the information system classification level. The information system classification level determines which network security zone the information system must reside.

7.8 - Mobile computing and teleworking

Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.

a) Information protection

Information Custodians must ensure that use of portable storage devices is managed and controlled to mitigate the inherent risks of portable storage devices.

The use of portable storage devices such as laptops or other mobile devices to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity a Security Threat and Risk Assessment must be performed prior to permitting subscription or use of mobile computing services.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

Providers of mobile computing services must perform annual risk assessments to identify service-specific risks. Policies, standards, practices and guidelines that treat these risks must be developed, documented and maintained.

b) Human factors

Information Custodians must provide users of mobile computing services with security awareness training, to ensure that users are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using portable storage devices;
- Aware that data is to be stored on Commission servers and accessed via mobile computing devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with the reporting procedure for lost or stolen devices.

c) Risk assessment factors

The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of the portable devices to remotely access Commission networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information classification and sensitivity levels must be considered in the risk assessment.

Minimum information protection safeguards for the use of portable storage devices include:

- Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a portable storage device must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on portable storage devices using Commission backup facilities to protect against information loss;
- To provide information availability portable storage devices must not be used to store the only copy of a Commission record;

- Physical security of the device must be maintained to protect against asset and information loss; and,
- User authentication to the portable storage device and user authentication for remote access from the device must be implemented in accordance with authentication policies.

d) Teleworking security controls based on risk assessment

Information Custodians must ensure that Commission information and information technology assets are adequately protected by implementing security controls supported by a Security Threat and Risk Assessment prior to granting permission for employees to enter into a teleworking arrangement.

The Security Threat and Risk Assessment must consider:

- The sensitivity and classification of information that may be accessed or stored at the teleworking location;
- The physical security of information, information technology assets and the teleworking location;
- Unauthorized information access by people at the teleworking location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.
- Security controls that must be considered include:
- Restriction of permitted information types and classifications at the teleworking location;
- Use of secure cabinets, shredders and other physical security equipment;
- Encryption of data stored at the teleworking location;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and,
- Monitoring and review of teleworking equipment for security events and incident response.

e) Teleworking agreement

Teleworking arrangements must be formally authorized and documented.

A documented teleworking agreement between the employer and employee must exist that specifies the following user responsibilities, terms and conditions:

- The expectation that the user will actively protect information and information technology assets;
- Restrictions on the information types or classifications permitted at the teleworking location;
- The requirement to protect information from inadvertent or deliberate disclosure to people at the teleworking location by use of secure cabinets, passwords or shredders;
- The authorized teleworking location and contact information;
- Information backup requirements;
- What equipment and software is supplied by the employee and what is supplied by the employer;
- The terms of use for remote access, if applicable;
- The requirement to meet or exceed specified wireless networking security controls, if wireless networking will be used at the teleworking location;
- The requirement to report security events or unusual activity;
- The right of the province to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking;
- The requirement to establish and maintain security controls as determined in the Security Threat and Risk Assessment;
- Arrangements for technical support; and,

- The start date, end date, expected work hours and provision for termination of the teleworking arrangement.

f) Ad hoc teleworking policy

Controls required for ad hoc teleworking are:

- Restriction of the information types and classifications that may be accessed or utilized while teleworking;
- Use of the Commission secure VPN access;
- If required, use of a Commission terminal server;
- Use of SSL Commission websites (e.g.; webmail, ESS);
- Minimum technical security controls required for non-Commission computing equipment, in particular current anti-virus, personal firewall and current software patches; and,
- Subject to applicable law, the right of the Commission to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking.

Chapter 8 - Information Systems Development and Maintenance

This chapter establishes requirements for incorporating security measures into the life cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

8.1 - Security requirements for information systems

a) Security controls for information systems

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information Custodians must conduct a Security Threat and Risk Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Work with the Information Owners to assign a security classification to the information and information system.

The Information Custodian must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common security processes and services (e.g., authentication, access control, financial management).

b) Security requirements at implementation

Information Custodians must ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing the requirements stated in the system security plan.

c) System Security Plan

A System Security Plan must be documented and maintained for each information system.

The System Security Plan includes:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for information system security management;
- Specific procedures and standards used to mitigate risks and protect the information system;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures.

8.2 - Correct processing in applications

a) Input data validation

Data input to an information system must be validated to ensure that it is correct and appropriate. Information Custodians must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and;
- Using control balances to verify complete input and processing.

d) Internal processing

Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity. Information Custodians must require that information systems include internal processing checks to:

- Detect unauthorised or incorrect changes to information;
- Prevent information from being accidentally overwritten;
- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);
- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;
- Maintain audit trails; and,
- Provide error and exception reports.

e) Message integrity

Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content. Information Custodians must determine message integrity requirements during the requirements definition phase of system development or acquisition.

Message integrity controls may include:

- Cryptographic signing; or,
- Checksum or hash functions.

f) Output data validation

Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Information Custodians must require that processes are documented to validate the data output from an information system by:

- Reconciling control balances to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, precision and classification of the information;
- Maintaining audit trails; and,
- Providing error and exception reports.

8.3 - Cryptographic controls

The use of cryptographic controls must be based on the risk of unauthorized access and the classification of the information or information system that is to be protected.

a) Roles and responsibilities

The IT department is responsible for the provision of cryptographic services, such as those used for user registration services and key management services, by:

- Establishing policy and providing strategic direction on the use of cryptography;
- Setting standards for cryptographic algorithms and key length;
- Defining where cryptography must be used;
- Approving the use of cryptographic services;
- Defining and maintaining standards for cryptographic controls; and,
- Providing technical advice on the use of cryptography.

Information Custodians must document the use of cryptography in the System Security Plan for the information system.

b) Acceptable use of cryptography

The type and quality of cryptographic controls used in information systems must be based on a Security Threat and Risk Assessment, and include consideration of:

- Confidentiality requirements, in accordance with information classification, labelling and handling requirements;
- Integrity requirements (e.g., for financial payments, personal information);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for proof of origin, receipt, or ownership);
- Legislation, regulations or policies requiring the use of cryptography;
- Restrictions on the export or use of cryptographic products; and,
- Risks relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

c) Management of cryptographic keys

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls.

The Senior Network Security Analyst is responsible for managing key management standards and processes, including:

- Selection of cryptographic keys with sufficient lengths;
- Distribution, storage and periodic updating of cryptographic keys;
- Revocation of cryptographic keys;
- Recovery of cryptographic keys that are lost, corrupted or have expired;
- Management of cryptographic keys that may have been compromised; and,
- Management of certificate authorities.

8.4 – Security of system files

The implementation of software on operational information systems providing services must be controlled.

a) Changes to operational information systems

Information Custodians must implement procedures to control software installation on operational information systems providing services to ensure that:

- Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- Operations personnel and end users have been notified of the changes, potential impacts and if required have received additional training;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to operational software are logged;

- The number of personnel able to perform the updates is restricted and kept to a minimum;
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

b) Pre-Implementation guidelines

Before an updated or new information system is implemented into the operational environment, checks should be performed to ensure that:

- A Security Threat and Risk Assessment has been carried out;
- Security hardening testing (e.g.; penetration testing, Nessus scanning);
- A Privacy Impact Assessment has been performed;
- Limitations of security controls are documented;
- Performance and capacity requirements can be met and have the capacity to maintain the information system;
- Development problems have been resolved successfully;
- The effects on existing operational information systems are known; and ,
- Arrangements for fall-back have been established if the updated or new information system fails to function as intended.

Steps to perform before the updated or new information system is implemented into the operational environment include:

- Communicate changes to users who may be affected by the change;
- Error recovery and restart procedures should be established;
- Disaster Recovery plans should be developed or updated;
- Operating procedures should be tested;
- Users should be educated to use the information system correctly and securely; and,
- Computer operator's/system administrators should be trained in how to run the information system correctly and securely.

c) Implementation guidelines

The installation process should include:

- Validating the load or conversion of data files;
- Installing executable code only, and not source code;
- Providing ongoing technical support;
- Implementing new or revised procedures/documentation;
- Discontinuing old software, procedures and documentation;
- Arranging for fall-back in the event of failure;
- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and,
- Recording installation activity and documenting in the DRP.

d) Post-implementation guidelines

Post-implementation reviews should include:

- Security hardening re-testing (e.g.; penetration testing, Nessus scanning);
- Lessons learned and scope for improvements of security controls; and,
- Security incidents and mitigation.

e) Protection of program source libraries

Access control must be maintained for program source libraries. Information Custodians must implement procedures to control access to program source code for information systems that include:

- Program source code is isolated and stored separately from operational information systems;
- Program source code is contained in protected code repository;
- Privileged users access is defined and monitored;
- A change control process is implemented to manage updating of program source libraries and associated items; and,
- Accesses and changes to program source libraries are logged.

8.5 - Security in development and support processes

Changes to software must be controlled by the use of formal change control procedures.

a) Changes to software during information systems development

Information Custodians must implement a change control process during development which includes:

- Requiring that change requests originate from authorized personnel;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

b) Changes to software for operational information systems

Information Custodians must implement a change control process during the maintenance phase including:

- Requiring that change requests originate from authorized personnel;
- Performing an impact assessment considering items such as the System Security Plan and proposed modifications;
- Documenting fallback plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating the System Security Plan and other system, operations and user documentation with the details of changes in accordance with records management policy;
- Maintaining version control for all changes to the software; and,
- Logging all requests for change.

c) Changes to the operating system

Information systems must be reviewed and tested when operating system changes occur.

Information Custodians must account for:

- Sufficient time for the review and testing of information systems prior to implementation;
- Review of System Security Plans to ensure information systems will not be compromised by the change;
- Information system testing with the changes to the operating system in a separate (i.e. test, stage) environment if and environment exists;
- A roll back plan in the event of change failure; and,
- Update of disaster recovery plans if required.

d) Changes to commercial-off-the-shelf software

Other than vendor supplied patches, commercial-off-the-shelf software must not be modified except in exceptional circumstances when needed for a critical business requirement. This requirement must be documented and approved by the Information Custodian.

A software update management process must be maintained for commercial-off-the-shelf software to ensure the most up-to-date approved patches have been applied and the version of software is vendor supported.

e) Preventing information leakage

Controls must be applied to limit opportunities for information leakage. Information Custodians must implement processes to reduce the opportunity for information leakage in information systems by:

- Scanning for malicious code;
- Monitoring resource usage in information systems;
- Monitoring for unusual access in information systems;
- Identifying and limiting the trusted connections in and out of the Commission network;
- Controlling third party network connections (e.g., only authorized traffic permitted);
- Using software that is considered to be of high integrity; and,
- Regular monitoring of information systems.

f) Outsourced information system development

Controls must be applied to secure outsourced information system development. Information Custodians must consider the following when outsourcing information system development:

- Procurement policy for licensing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Testing of the information system for common vulnerabilities and malicious code;
- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

8.6 - Vulnerability management

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

a) Vulnerability response processes

Vulnerabilities which impact Commission information systems must be addressed in a timely manner to mitigate or minimize the impact on operations. Information Custodians must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities;
- Weekly automated scanning of systems with a vulnerability assessment tool (e.g.; Nessus scanner);
- Assessing the risk of published vulnerabilities;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- Applying corrective measures to address the vulnerabilities; and,
- Reporting to the any found vulnerabilities.

The Senior Network Security Analyst must:

- Evaluate vulnerabilities and provide advice on appropriate responses;
- Monitor progress in responding to vulnerabilities;
- Publish summary reports on vulnerability response activities; and,
- When required, initiate incident response processes to address vulnerabilities.

Chapter 9 - Information Security Incident Management

This chapter establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that personnel understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the Commission.

9.1 - Reporting information security events and weaknesses

a) Reporting information security events

Commission personnel and contractors must immediately report all suspected or actual information security events to the IT Department as required by the Information Incident Management Process. Requirements for reporting events must be included in contracts and service agreements.

Information security education for Commission personnel should build trust with users and stress that "to err is human". Positive reinforcement of good reporting practices will help users understand their responsibilities. Users who commit errors that lead to security incidents should receive appropriate training to help prevent future incidents

b) Reporting security weaknesses

Commission personnel and contractors using information systems must note and report any observed or suspected security weaknesses in those systems to help assist in maintaining the security of the systems.

Information Custodians must follow the Information Incident Management Process for responding to suspected or actual security weaknesses which includes:

- Ensuring all reports are investigated and handled in a secure, confidential manner; and,
- Ensuring the individual who reported the weakness is advised of the outcome when the investigation is complete.

9.2 - Management of information security incidents and improvements

a) Information security incident management and response

The IT Department must follow the Information Incident Management Process for reporting, managing, responding to and recovering from information security incidents. The process must include:

- A reporting process that includes the Senior Network Security Analyst;
- When exercising incident management authority, authorized staff must notify senior management of the incident and mitigation activities at the earliest possible time;
- Staff with incident management responsibilities must be appropriately trained and qualified, and their authorization for access to live systems and data delineated formally;
- Processes are established for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans; and,

- Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

b) Information security incident investigation

Information security incident investigation should be formalized and practiced in accordance with standard investigation techniques:

- Information security incident investigation processes include:
  - Identification of the incident's cause,
  - Planning of corrective action,
  - Implementation of corrective action to prevent recurrence, and,
  - Post-mortem - Reporting action taken;
- Staff with responsibilities for information security investigations (Senior Network Security Analyst) must be aware of processes for securing potential evidence such as technology assets (e.g., PCs), audit logs, audit trails, voice mail and e-mail accounts for analysis and as potential evidence in legal proceedings;
- Inappropriate use of information and technology resources requires that within 48 hours the investigating officer contact:
  - In the case of an employee the individual's excluded Manager, and,
  - In the case of a contractor or business partner the contract manager.
- When criminal activity is suspected, the investigating officer must ensure that the appropriate law enforcement authorities are contacted. However, before contacting law enforcement authorities the Risk Management Branch and Government Security Office and the Office of the Government Chief Information Officer must be consulted;
- On resolution of an information security incident or weakness, the investigating officer must prepare a report that includes a detailed problem analysis, action(s) taken, and recommendations for corrective action or improvements; and,
- Information security incident reports must be submitted to Information Owners, Information Custodians and senior management as part of security program management.

c) Learning from past incidents

Continuous improvement of security incident management processes includes:

- Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- Analysis of incidents, responses and successful containment;
- Determining requirements for user awareness and training;
- Improving the security of information systems through monitoring and reporting;
- Integrating automated alarms and other security incident detection technology with user reporting, checking logs and auditing systems; and
- The consolidating of reporting for all security weaknesses, threats, events and incidents to avoid duplication and establish a consistent approach.

Personnel who regularly ignore policy should be subject to a disciplinary process that includes notification of their manager and suspension of privileges for repeated offences.

d) Monitoring for security breaches

The Senior Network Security Analyst is responsible for monitoring for and evaluating information security incidents by:

- Using statistical analysis of incident frequency, type and location to identify trends;
- Ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and business continuity and disaster recovery plans;
- Advising Information Owners and Information Custodians of evolving security exposures and mitigation strategies;
- Evaluating the effectiveness of incident management, response and reporting; and,
- Evaluating the effectiveness of information security technologies.

Potential types of security incidents to be reported include:

- Breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code (e.g., virus, worm, Trojan Horse);
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing; and,
- System failures and loss of service.

e) Collection of evidence

Investigations into information security incidents must ensure evidence is collected, retained and presented. At the outset of an information security investigation it may not be known if legal or disciplinary actions will result. Evidence must only be collected by individuals authorized by the Commission senior management.

Evidence collection procedures must be documented by the Senior Network Security Analyst.

Investigative processes must follow the rules of evidence to ensure relevance, admissibility and materiality.

Information Owners and Information Custodians in receipt of a legal order to produce electronic evidence must immediately contact the Senior Network Security Analyst.

Chapter 10 - Disaster Recovery & Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a major disruption has occurred. The Commission is required to be prepared and to re-establish business or services as swiftly and smoothly as possible. Development and review of these plans include the evaluation of security risks.

10.1 - Information security aspects of Disaster Recovery and Business Continuity management

a) Disaster Recovery

When developing new documentation to be part of the DRP, each new document must be reviewed for security considerations. There are several sections of the DRP that are reviewed/revised yearly by IT Security staff including (but not limited to) firewall, third party gateway, VPN, etc.

b) Business continuity

During each year's annual review of the BCP if there are major changes to the core of the document it must be evaluated by IT Security staff. The purpose of the review is to determine if there are risks associated with implementing the BCP and create a mitigation plan.

Chapter 11 - Compliance

The chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the Commission is in compliance with applicable laws and policies. Processes to monitor the extent in which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

11.1 - Compliance with legal requirements

The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.

a) Legal requirements

Information Custodians are responsible for ensuring that statutory, regulatory, policy and contractual requirements of each information system are:

- Identified and documented when commencing a system development or enhancement initiative;
- Reviewed prior to, or concurrent with, changes to legislation, regulation or policy; and,
- Explicitly identified in contracts and service agreements, and included in:
    - Privacy Impact Assessments,
    - Security Threat and Risk Assessments,
    - System Security Plans,
    - Risk Management Plans, and,
    - Business Continuity Plans.

Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing.

b) Intellectual property rights of external creators and owners

Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing.

Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licenses;
- Requiring the removal of unlicensed information and software from Commission information systems;
- Informing personnel of Commission policies including those pertaining to appropriate use of Commission resources;
- Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- Complying with terms and conditions for information and software obtained from public networks (e.g., "free for personal use only", open source).

c) Records management

To ensure the Information Security Policy and supporting processes enable compliance with legal and policy requirements for government records, Commission records must be protected from loss, destruction and falsification.

The Document Disposal Act defines requirements for the disposal of government records.

Policy requirements for records management are in Core Policy and Procedures Manual 12.3.3 - Information Management, and the Commission's internal Records Management Policy

d) Data and personal information protection

The Freedom of Information and Protection of Privacy Act requires personal information to be protected using 'reasonable security measures'.

Policy requirements for protecting data and personal information are found in Core Policy and Procedures Manual 12.3.3 - Information Management and the Freedom of Information and Protection of Privacy Act Policy and Procedures Manual.

This Information Security Policy includes detailed controls which enable and support the protection of Commission information and information systems.

e) Deterring unauthorized and inappropriate use of information systems

Controls must be in place to deter misuse of information systems. Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;
- Implementing processes to analyze audit logs to identify potential misuse of information systems;
- Implementing system rules to prevent access to undesirable Internet sites;
- Implementing content inspection and filtering tools (e.g., for e-mail and web traffic);
- Immediately notifying personnel of detected misuse (e.g., Websense for Internet blocking);
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining, in consultation with management, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for personnel who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes Information Custodians must ensure:

- Monitoring activities will be compliant with legal, policy and contractual requirements and obligations;
- Personnel are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a 'need to know' and 'least privilege' basis to the fewest possible number of users.

f) Regulation of cryptographic controls

Cryptographic controls must be used in conjunction with relevant agreements, laws and regulations. When cryptographic controls are used, Information Custodians must:

- Ensure that the use of cryptographic control(s) is supported by an Information Security Threat and Risk Assessment;
- Consult with the Senior Network Security Analyst regarding the records management, electronic commerce, information access, privacy and security issues prior to acquiring cryptographic controls;
- Ensure encrypted Commission information assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys; and,
- When acquiring cryptographic controls from outside Canada, the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into Canada.

The Senior Network Security Analyst will:

- Develop and document cryptographic key management processes;
- Provide guidance and assistance to Information Custodians in the selection and use of cryptographic controls; and,
- Establish and publish cryptographic standards.

11.2 – Compliance with security policies and standards

a) Compliance roles

Management must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.

Information Custodians must ensure security policies and processes are implemented and adhered to by:

- Conducting periodic self-assessments;
- Ensuring personnel receive regular information security awareness updates; and,
- Initiating independent assessments, reviews or audits to assess compliance to policy.

When review processes indicate non-compliance with policies, Information Custodians must:

- Determine cause(s);
- Assess the threats and risks of non-compliant processes; and,
- Develop plans to implement corrective action.

b) Review of controls

The Commission must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year. Mission critical information systems are to be reviewed at least annually.

c) Review of implementation of information incident report recommendations

Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

The Senior Network Security Analyst may perform compliance reviews or audit of the implementation of recommendations from information incident reports, when necessary. Information Custodians must support the audit activities.

d) Technical compliance checking

Information Custodians or the Senior Network Security Analyst must regularly test information system technical control compliance by using automated tools to:

- Detect network intrusion;
- Conduct penetration testing;
- Determine if information system patches have been applied;
- Confirm that system technical controls have been implemented and are functioning as designed; and,
- Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

Personnel responsible for technical compliance checking must ensure that:

- Affected Information Custodians, Information Owners and operations personnel are consulted prior to initiating tests; and,
- The Information Custodians responsible for monitoring are notified prior to testing to prevent triggering false security alarms from the infrastructure.

e) Reporting results

Managers responsible for technical compliance checking and Information Custodians must:

- Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Senior Network Security Analyst;
- Provide Information Owners and the Senior Network Security Analyst copies of test results and action plans;
- Provide the Senior Network Security Analyst with the internal or external audit reports immediately upon receipt; and,
- Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

11.3 Information systems audit considerations

Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.

a) Management of information systems compliance checking

Prior to commencing compliance checking activities such as audits, risk and controls reviews, monitoring or security reviews of operational information systems, the Manager responsible for the compliance checking activity, Information Custodians must define, document and approve the activities by:

- Determining the scope, duration and level of detail of the compliance checking activity;
- Limiting access rights to operational information systems for compliance checking personnel to "read only";
- Determining handling requirements for copies of files made by compliance checking personnel including:
    - Establishing a separate environment for the analysis of files,
    - Restricting access to those files,
    - Logging the accesses made to those files, and,
    - Erasing files at the conclusion of compliance checking activities unless needed to support report findings;
- Identifying special testing or processing which may impact the operational information system (e.g., penetration tests, server vulnerability assessments) and by:
    - Notifying the Senior Network Security Analyst prior to compliance checking activities to prevent triggering false security alarms from the infrastructure, and,
    - Scheduling tests to minimize disruption;
- Submitting the reports of penetration tests or vulnerability assessments to the Senior Network Security Analyst immediately upon receipt.

b) Protection of information system audit tools

Access to system audit tools must be controlled to prevent misuse or compromise. Managers responsible for compliance checking activities and Information Custodians must control the use of audit tools by:

- Restricting access to authorized personnel who have a need-to-know;
- Installing or enabling specialized audit tools for the duration required by the compliance checking activity;
- Removing information system access at the conclusion of the compliance checking activities; and,
- Notifying the Senior Network Security Analyst prior to the use of audit tools.

Glossary

Accreditation - the final approval to authorize operation of an information system and to explicitly accept the risk to Commission operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed upon set of security controls.

Ad hoc telework - occasional telework that may not have a formal agreement in place. (See: telework)

Application (business application) - a collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

Assets - for the purposes of information security policy, information in all forms and media, networks, hardware, software and application systems.

Audit - is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

Audit logs - includes all types of event logs including (but not limited to) security, audit, application, access and network across all operating system platforms.

Authentication - the verification of the identity of a person or process.

Availability - information or information systems being accessible and usable on demand to support business functions.

Business Continuity Plan (BCP) - the procedures and information necessary for the timely recovery of essential services, programs and operations, within a predefined timeframe. The BCP includes the recovery following an emergency or a disaster that interrupts an operation or affects service or program delivery.

Business information systems - internal administrative and productivity information systems that support the organization such as e-mail, calendars and financial systems.

Capacity management - the process of determining the system capacity needed to deliver specific performance levels through quantification and analysis of current and projected workload.

Certification - See: security certification

Commercial-off-the-shelf (COTS) - commercially available products that can be purchased and integrated with little or no customization.

Compliance checking - in the context of the Information Security Policy, includes: an audit; risk and controls review; security review; and monitoring of an information system.

Confidentiality - information is not made available or disclosed to unauthorized individuals, entities or processes.

Control - (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure. Where the information in a record directly relates to more than one public body, more than one public body may have control of the record.

Control balances - computational aids for data verification e.g., records counts, row and column counts, subtotals, etc.

Cryptographic Keys - a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of data into encrypted data and the transformation of encrypted data into data during decryption. The cryptographic algorithm ensures that only someone with knowledge of the key can reproduce or reverse the transformation of data.

Cryptography - the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.

Custody - (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.

Data - See: Information.

Diagnostic Ports - ports, services and systems used for diagnostic, maintenance and monitoring activities for managing information system performance, function or capacity. Examples include: physical network switch diagnostic ports, logical management services such as SNMP and modems for remote maintenance.

Digital signing - refers to an attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users' private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user's public key. (Also digitally signing, digital signature)

Disaster Recovery Plan (DRP) - the procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment. The DRP is part of a Commission's overall business continuity plan (Business Continuity Plan or BCP).

Disposition - the actions taken regarding information that is no longer needed to support on-going administrative and operational activities in accordance with an approved Records Management Schedule. Directions may include destroy, transfer to the government archives, transfer to inactive records storage space, or retain permanently in unit.

Electronic agent - a computer program, or other electronic means, used to initiate an activity or to respond to electronic information, records or activities in whole or in part without review by an individual at the time of the response or activity.

Electronic commerce - the exchange of information between government and internal and external stakeholders independently of either participant's computer system. E.g., electronically accessing forms, obtaining payments, sending invoices, receiving tax returns, placing orders and receiving transaction acknowledgements.

Electronic messages - includes all forms of electronic messaging such as e-mail, voice mail, instant messaging etc.

Employee - is a person employed by the Commission.

Essential services - Essential business processes are those processes defined as mission-critical and business- priority and essential to delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each essential business process.

Event - is an identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

External Party - a person external to the Commission.

Fault - an error or failure in either software or hardware.

Firmware - programming that is inserted into programmable read-only memory becoming a permanent part of a computing device.

Hardware - includes (but not limited to) servers, desktop computers, printers, scanners, fax machines, photocopiers, multi-function devices, routers, communications and mobile equipment, cell phones, mobile devices, removable media.

Information - the data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision making.

Information asset - includes all data, information and intellectual property.

Information classification label - a designation indicating the information classification, e.g., "Public", "Confidential", "Internal Only".

Information Custodians - maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. Information Custodians are staff in the Commission IT or IS Department.

Information labelling - affixing a physical or electronic label identifying the security category of a document, file or records series in order to alert those who handle it that it requires protection at the applicable level.

Information Owners – the person with the primary responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

Information processing facilities - the physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

Information Security - preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Information security activities - management and technology programs to protect government information assets.

Information security architecture - a strategy that consists of layers of policy, standards and procedures and the way they are linked to create an environment in which security controls can be easily established.

Information Security Classification - a system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability. (also classification, information classification, security classification)

Information Security Event - See: event.

Information Security Incident - is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (ISO/IEC TR 18044:2004) Information security incidents may include but are not limited to:

- Inappropriate use of government resources causing a service disruption;
- Breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code, e.g., virus, worm or Trojan horse;
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing;
- System failures and loss of service.

Information System - any equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

Information System Security Classification - a system of designating security categories for information systems based on the information security categories of information processed by the information system.

Information technology asset - includes owned and leased technology hardware (i.e. physical items), owned or licensed software and related or supporting services.

Information technology resources - information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

Information type - information classes or groupings based on function, usage, attributes or other commonality. E.g., personnel records, invoices, or system documentation are information types. Address, name, or birth date are examples of discrete data elements.

Integrity - the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

Intellectual property - intellectual property refers to the category of intangible (non-physical) property consisting primarily of rights related to copyrighted materials, trademark, patent and industrial design.

Intellectual property rights are associated with a wide range of products of the human intellect, such as training manuals, publications, map products, videos and computer software. It is important to keep clear the distinction between the items that give rise to intellectual property, such as the manuals and software, and the intellectual property itself, which is the set of rights arising from the creation and development of the items. Simply put, the items are the copies of a particular book, whereas the intellectual property is the copyright in that book.

Key Management - the processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys.

Least Privilege - a security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Malicious code - malicious code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code can include viruses, worms, Trojans, spyware and denial of service attacks.

Media - Material that information is written to and stored on. See: Records.

Message integrity - the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient to maintain the completeness, accuracy and validity of the information contained in the message.

Mission Critical - processes that, should they not be performed, could lead to loss of life ("safety"), personal hardship to citizens, major damage to the environment, or significant loss in revenue and/or assets.

Mobile code - multiplatform computer code that can be downloaded or transmitted across a network that runs automatically on a computer with little or no user interaction.

Mobile code technology - software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, VBScript, ActiveX).

Mobile computing service - a service that provides access to government systems from Mobile Computing Devices. Distinct from Remote Access Services in that the mobile computing service provides product-specific access to limited applications rather than full standard network access (e.g., Exchange ActiveSync Service).

Mobile devices - portable self-contained electronic devices, including portable computers (e.g., laptops), personal digital assistants (PDAs), cell phones, digital cameras, etc.

Monitoring - a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.

Multi factor authentication - this is combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret - something the person knows Token - something the person has Biometric - something the person is.

Need to know principle - a privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office. The need- to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems. The need-to-know principle is especially important in protecting the privacy of individuals as required by the Freedom of Information and Protection of Privacy Act.

Network Address Spoofing - forging or faking source network addresses with the intent to obscure, hide or impersonate the actual source device.

Network infrastructure - the equipment, information systems and cabling systems used to establish a communication network between Information Systems. Includes routers, switches, hubs, firewalls, transmitters, fibre optic cable and copper cable.

Network management information - the information used to manage network infrastructure, including traffic statistics, counters and logs.

Network pathways and routes - the physical and logical pathways that comprise the connections within the network infrastructure.

Network security boundary - the logical or physical boundary between networks of differing security protection requirements. Network access control devices demark the network security boundaries.

Network security zone - a logical entity containing one or more types of services and entities of similar security requirements and risk levels.

Network segregation - the separation of groups of users, information systems and services with similar business functions by control of network traffic flow, e.g., by use of security gateways, physically separate networks or access controls.

Network service agreement - The contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery.

Network service provider - a provider of network services to the Commission which may be internal or external to government.

Non-repudiation - the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Non-retrievable - unable to recover the data from any media in any form.

Outside authorities - include law enforcement, fire departments, other emergency response authorities, utilities and telecommunications providers.

Password management system -An automated process which enforces password rules.

Personnel - includes employees and other individuals (e.g., contractors, consultants, volunteers, third-party organizations).

Portable storage devices - electronic media including but not limited to laptop and notebook computers, removable hard drives, USB mass storage devices (flash drives, jump drives, memory sticks, memory cards, thumb drives, MP3 players, iPODs and PDAs), zip drives, CDs, DVDs, tapes and diskettes.

Positional user identifier (userid) - is a unique system userid assigned to a persistent function or job in circumstances where the personnel filling the job are transitional. Positional userids are issued to a Manager or supervisor who is accountable for the day to day management and assignment of the userid to individuals. E.g., a positional userid could be used if a receptionist position was temporarily filled by short term staff from an employment agency. In these limited circumstances use of positional userids can avoid creating new userids for short term staff.

Privacy - the right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents.

Privacy Impact Assessment - an assessment that is conducted to determine if a new enactment, system, project or program meets the requirement of Part 3 of the Freedom of Information and Protection of Privacy Act.

Privileged operations - permissions which allow the user to alter access rights and structures of information systems and/or services.

Privileged users - users with permissions to alter access rights and structures of information systems. This includes (but is not limited to) system administrators, network administrators, database administrators, security administrators, web site administrators, system operators and network operators.

Privileges - See: privileged operations.

Reception Zone - an area where the initial contact between the public and the Commission occurs, where services are provided, information exchanged and access to restricted zones is controlled.

Record - includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.

Remote access - the act of using a remote access service to connect to the Commission network or government systems.

Remote access service - a service that provides network access to the Commission network or Commission systems from a remote location, e.g., the VPN service.

Requirements phase - one component of the System Development Life Cycle. Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable, testable and related to the business need or opportunity.

Restricted Access Operations Zone - a controlled area where access is limited to persons who work there and to escorted visitors. It is usually a standard working area and offices.

Restricted Access Security Zone - a strictly controlled area where access is limited to authorized persons and to properly escorted visitors.

Risk - Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

Request BCER2024-003 - Page 139 of 260

Risk and controls review - an independent and objective assessment of an information system to determine whether the business/system framework has adequate controls to mitigate business, financial, security and general privacy risks.

Screening - to verify facts about individuals related to their identity, professional credentials, previous employment, education and skills.

Secured Path - a network path that has been protected from eavesdropping, intrusion and data tampering.

Security categories - inform employees how to handle records in order to protect them and determine requirements for marking, storage, transport, transmittal and destruction.

Security certification - a comprehensive assessment of the management, operational and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security infrastructure - the complete set of information security-related systems, policies, standards, guidelines, procedures, resources and physical implementations of information security administration.

Security Management Systems - systems that collect, store and manage configuration and operational information about network devices. Includes configuration management databases and log management systems.

Security posture - the security status of the technical infrastructure and information systems to known vulnerabilities and attacks.

Security review - an independent review with the scope focused on the security framework over the business processes, application and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.

Security Threat and Risk Assessment - a component of a risk analysis specifically aimed at identifying security exposures.

Security weakness - a weakness in an application, procedure or process that may result in a security incident.

Security zone - See: reception zone, restricted access operations zone, restricted access security zone.

Software - includes (but not limited to) application and system software, development tools, utilities.

Status Accounting - a comparison of configuration data stored in a configuration database to actual device configuration. Used to ensure that recorded configuration data matches actual device configuration.

System Security Plan - repository to document security information and controls (management, operational and technical) regarding an application system.

System Utility Programs - Tools that when misused can subvert system, access and application controls E.g. network sniffers, password crackers, port scanners, root kits and vulnerability assessment scanners.

Systems documentation - detailed information about a system's design specifications, its internal workings, and its functionality including schematics, architectures, data structures, procedures and authorization processes.

Systems privileges - permissions which allow the user to alter access rights and structures of information systems.

Telework - a working arrangement where employees work away from their official workplace for a portion of their regular work week (Flexible Work Options). (See: ad hoc telework)

Third party - includes external party and includes a person outside the direct reporting structure of the Information Owner or Information Custodian. E.g., an individual, a business or organization, personnel from another branch of government, or another level of government.

Threat - in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin. (See: vulnerability and event).

Trusted path - See: secured path

Two person access control - a system of requiring the presence of two authorized persons to perform an action, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. For example, a locked cabinet or safe which has two locks requiring action by two persons, each with a unique key or code and which requires the presence of two persons to access or open.

Uninterruptible power supply - a backup power source for computers and computer networks to insure on-going operation in the event of a power failure.

User - all persons authorized to access the Commission's internal bcogc.local domain in any capacity including employees and contractors.

User identifier - is the unique personal identifier that is authorized to access the Commission's computer and information systems.

Vulnerability - in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Wireless Local Area Network - a Local Area Network that uses wireless transmission media, such as 802.11a/b/g/n or WiMax.

Zone - See: reception zone, restricted access operations zone, restricted access security zone.

ISSUANCE: **Corporate Services Division**
Records Management/Information Technology

APPROVED: **April 27, 2021**

1.0 GENERAL

1..1 Background

The BC Oil and Gas Commission (Commission) is adopting Microsoft Office 365 (M365) as a communication, collaboration and working platform. M365 provides a new suite of tools for creating, accessing, and sharing information and creates new digital workspaces.

1..2 Purpose

The purpose of this policy is to set a standard for how the Commission will use the M365 applications and appropriately manage the information residing in them. The use of M365 tools must comply with our legislative and policy requirements relating to information management and confidentiality. This means records and information stored using an M365 application or service must be:

- Appropriately retained to adequately document Commission decisions.
- Actively managed throughout their lifecycle according to retention policy.
- Secured and managed to prevent inadvertent disclosures.
- Assessed for confidentiality and, when appropriate, protected as a confidential asset.
- Readily accessible for Freedom of Information (FOI) and eDiscovery requests.

M365 is a new digital platform for the Commission and the Province, and its suitability as a corporate recordkeeping system has not yet been fully assessed. As such, this policy is deemed interim in nature and may be subject to future revisions.

- **Authorities**
  - *Information Management Act*
  - *Interpretation Act*
  - *CRO 01-2019 Documenting Government Decisions Directive*
  - *Freedom of Information and Protection of Privacy Act* (FOIPPA)
  - *Transitory Records (Schedule 102901)*
  - *Oil and Gas Regulation Operational Records Classification System (ORCS)*
  - *Administrative Records Classification System (ARCS)*
  - *Human Resources ARCS Supplement*

- **Applicability**

  This policy applies to all data, records and information stored in M365 applications.

- **Related Policy/Procedure**

  This policy, in conjunction with the following, is part of the information governance framework in the Commission:

  - *Information Management Policy*
  - *Managing Confidential Information Guide*
  - *Managing Email Guide*
  - *Employee Code of Conduct and Ethics*
  - *Information Security Policy*
  - *Mobile Device Policy*
  - *Use of IT Resources Policy*

2.0 POLICY

2.1 Records and Information Management

- Commission records and information must be consistently managed according to approved information schedules (i.e., ARCS/ORCS).
- Official records within M365 workspaces must be saved to an appropriate recordkeeping system (shared drives) to ensure Commission decisions are adequately documented and business continuity and operations are supported.
- Only transitory information may be destroyed at the discretion of the employee.

2.2 Collaboration and Protecting Confidentiality

When using M365, users must limit the sharing of sensitive or confidential information, (e.g., personal information).

- Confidential records and personal information must not be inappropriately shared in M365 workspaces. If sharing is necessary, ensure proper handling and protections are in place.
- Access to M365 workspaces will only be granted to appropriate users and groups, as determined by Team/Site Owners.
- Access permissions assigned to collaborative workspaces will be actively managed, and access will be updated in a timely manner when group composites change.
- External individuals will not be granted access to Commission M365 workspaces without prior approval by a member of the Leadership group. If permissions are granted, Team/Site owners must ensure the protection of any confidential or sensitive information in the shared environment.

2.3 Freedom of Information and legal records searches (eDiscovery)

Information in M365, like all Commission information, is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or other legal obligations. When using M365, staff must be prepared to respond to Freedom of Information (FOI) and legal requests for records and information.

Upon notification of a FOI and/or legal discovery request, users must assist in the search and retrieval of responsive records from applicable M365 workspaces, within prescribed time allowances as requested by FOI or Legal Services branch.

- Employees must not delete responsive records or information stored within M365 workspaces, including that which may be considered transitory. It is unlawful to delete or destroy any transitory record that is the subject of a current FOI request, or is subject to a current or reasonably anticipated litigation discovery process.
- Temporary holds on M365 automated information deletions should be initiated for applicable M365 applications.
- Searches for responsive records must be conducted within all applicable M365 workspaces.

3.0 APPLICATION USAGE

3.1 Teams

Teams workspace is to be used for transitory information only.

Teams is used for:

- Ad hoc informal conversations (chats) between two or more people.
- Department/branch communications.
- Project/committee/working groups.

Retention of chat messages:

- Ad hoc chat messages (outside of Teams Sites and Channels) are automatically deleted after 10 days.
- Department/branch conversations (within a Teams Site or Channel) are automatically deleted after three months.
- Project/committee/working group conversations (within Teams Sites or Channels) are kept for the duration of the project, then deleted.

Documenting decisions and capturing official information in Teams:

- Any official or critical information in Teams must be captured in the recordkeeping system.
- Team/Site Owners must confirm that all official material has been transferred to the recordkeeping system before a Team site will be deleted.

3.2 OneDrive

OneDrive is similar to the F: drive, by providing a private workspace for individual use. It is intended for short-term storage of records being actively worked on, i.e., drafting and collaborating on new documents OneDrive is not an appropriate repository for long-term storage and management of Commission records.

OneDrive workspace should only hold active records while being drafted, and transitory information.

- When a record is finalized or collaboration has completed, it should be moved to the recordkeeping system.
- Users/Supervisors must confirm any official material has been transferred to the recordkeeping system before a OneDrive account is closed/deleted.

Confidentiality and collaboration considerations:

- Care must be taken to ensure that security and permissions are closely managed for confidential information being shared for collaboration.

3.3 SharePoint

There are two main uses of SharePoint in M365. Teams uses SharePoint as the platform for sharing and collaborating on documents – each Teams SharePoint is specific only to that Team and intended for short-term use and collaborative purposes. An official SharePoint site can also be used as a broader communication tool or collaboration hub at a corporate level; content stored on such sites is typically accessed across the organization and referenced for a period of longer duration, i.e., corporate policies and planning documentation, etc.

Teams SharePoint is a workspace for transitory content.

- Official records created within this workspace must be moved out of the Teams environment and saved to the recordkeeping system.

SharePoint sites outside of Teams are typically retained for a longer duration; as such, content must be managed according to records lifecycles and retention rules.

- Initiation of a corporate SharePoint site will be done in accordance with Commission SharePoint standards.
- Site structure must align with approved information schedule classifications.
- The Commission will actively maintain documentation on the intended use, access, and permissions for every site.
- SharePoint sites may be used as a records repository provided the structure aligns with information schedule classifications.
- When a site is closed, all official records should be extracted from SharePoint and saved to the recordkeeping system.

3.4 Outlook

M365 connects to Exchange Online instead of Exchange onsite. This does not significantly change email functionality or email management requirements.

- Emails should be managed according to information schedule classification and retention rules.
- Official emails should be routinely moved to and retained in the recordkeeping system.
- Inactive mailboxes may not be deleted until the contents have been assessed and official records are retained in the recordkeeping system.

4.0 ROLES AND RESPONSIBILITIES

Leadership is responsible for:

- Leading the Commission in the appropriate usage of M365 tools.

Teams/Site Owners are responsible for:

- Assigning and managing permissions to Commission workspaces.
- Ensuring the site or group workspace is appropriately managed according to Commission policy throughout its duration.

- Ensuring official records are captured in the recordkeeping system before a site/channel/group mailbox is closed.

Each employee is responsible for:

- Understanding what constitutes an official record and what information is deemed transitory.
- Managing Commission records and information, throughout the lifecycle established in approved information schedules, as appropriate to each M365 application.
- Ensuring appropriate confidentiality measures are applied to records and information.
- Ensuring the privacy of individuals is protected and maintained when using M365 tools and applications.
- Coordinating and/or conducting records searches within M365 applications in response to an FOI and/or legal request (eDiscovery).

APPROVAL:

Paul Jeakins
Commissioner,
Chief Executive Officer

Len Dawes
Executive Vice President,
Chief Financial Officer

Ken Paulson
Executive Vice President,
Chief Operating Officer

Mayka Kennedy
Executive Vice President,
Chief Engineer

Ines Piccinino
Executive Vice President,
Legal and Regulatory Affairs

Trevor Swan
Executive Vice President,
Orphan & Liability Management

Version Control:

Document Created	Apr-21	Approved by Executive Team

Appendix A: Definitions

- **Access:** the ability or opportunity to view, study or obtain a copy of the records of the Commission. FOIPPA provides the public with a right of access to records in the custody or under the control of a public body.
- **Classification:** the process of identifying records or information in accordance with an approved information schedule. This includes determination of the function and/or subject of a record and selection of the appropriate records classification.
- **Confidential Record/Information:** is information that, if compromised, could result in serious consequences for individuals, organizations, or government. Designating information as confidential depends on factors such as the value of the information, the source of the information, and the impacts of unauthorized use, disclosure, alteration, reproduction, loss, or destruction. Confidential information requires protection against unauthorized access or disclosure.
- **Outlook:** is Microsoft's email application in M365. It supports the creation and receipt of electronic mail communication.
- **Information Governance (IG):** is fundamental to good corporate governance. It provides a framework and foundation for the control and securement of corporate records and information. It relates to the activities, policies, processes, and technologies an organization applies to maximize the value of the information it holds, while minimizing the costs and risks associated with holding it. The Commission's M365 IG Policy identifies requirements and strategies for managing content and records throughout their lifecycle using the suite of tools. The focus is on being compliant with applicable legislation and policies and enabling employees to be more collaborative and productive.
- **Information Schedules**: govern how records are organized and managed. B.C. government and broader public sector organizations use information schedules to ensure records are kept for as long as required, identify records of enduring value for preservation and ensure others are routinely destroyed when they are no longer needed.
- **Leadership Group:** Commission employees with a designation of Executive Director or higher.
- **Lifecycle**: the lifespan of information from its creation or receipt and use, through to its final disposition: destruction, transfer to the government archives or alienation.
- **Official Record/Information:** a record that documents Commission activities and decisions and does not fit the criteria of transitory records.
- **OneDrive:** cloud-based storage provided to each employee for information and materials related to their work.
- **Personal Information**: is recorded information about an identifiable individual other than business contact information. Business contact information identifies an individual in a business, professional or official capacity, and can include their name, title, business address, business telephone number, business email or business fax number. Personal information typically includes an individual's name, home address, personal email address, personal telephone number, age, gender, marital or family status, any physical or mental descriptors, information about an individual's educational, financial, criminal or employment history, personal views or opinions, and photos where individuals are identifiable. A name is considered personal under FOIPPA when, combined with other personal

information, it reveals something personal about that individual. The context in which an individual's name appears determines whether it is personal information.

- **Records/Information Management**: is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Recordkeeping System:** a shared filing system in which records are captured, protected, retained, and destroyed in accordance with approved information schedules, and the integrity of the digital government information is ensured. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and ongoing training, constitutes an appropriate system for managing Commission information. Currently the Commission's recordkeeping system consists of shared drive folders.
- **Record/Information**: is created, received, and maintained by an organization or person during business. This includes formats defined in the Interpretation Act and FOIPPA, which includes "information that is recorded or stored by any means whether graphic, electronic, mechanical or otherwise".
- **Responsive Records/Information**: all records or information that pertain to the wording and/or subject of an FOI or legal request and fit within the scope of an applicant's request. A record may be deemed responsive as a result of its creation date, its content or context, who created the record, etc.
- **Retention Rules/Schedule:** embedded in Information Schedules, retention schedules govern the life cycle of a record, or series of records, provide the length of time the record is to be retained and its final disposition - destruction or transfer to the government archives.
- **SharePoint Site:** a central repository within M365 for information, links and content which may relate to a specific group of users for a specified purpose, or as a communication "hub" for an organization. SharePoint integrates with the other M365 applications and services and is intended for communication and collaboration.
- **Team's Site (referred to as a Team within Teams):** a collaborative workspace that provides transitory chat messaging, audio/video conferencing, document and information sharing, and meeting recordings. Team sites interface with a variety of M365 applications including Outlook, and documents residing in OneDrive and SharePoint. Teams Sites are structured with Channels, which are dedicated to a purpose.
- **Teams Channels**: dedicated conversation and workspace within Teams sites, where a group of people, such as project teams, committees, working groups, departments, and branches can collaborate and communicate.
- **Teams Chats (ad-hoc):** transitory instant messaging for the purpose of informal communication between people outside of Teams channels.
- **Team/Site Owner:** a Commission employee assigned as the owner of a Team who can create Channels within their team and manage permissions for those Channels. Additionally, Team Owners can set up properties for the Team including Team name and adding apps.
- **Transitory Information**: information of temporary and/or low value that is needed for only a limited period in order to complete a routine action or prepare a subsequent record (e.g., a new version). Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions.

- **Workspace**: a broadly used term referring to M365 digital platforms where we work with records and information, such as a Teams collaboration space, SharePoint site and/or OneDrive location.

Program Charter

Digital Information Management Program

DRAFT

Information Systems & Technology
October 2022

DRAFT

Program Overview

Section 13

Program Scope

Section 13

Section 13

Section 13

Program Stakeholders – Commission

Stakeholder	Program Interest / Expectations
Executive Committee	Assurance regarding objectives and efficacy of the DIM Program
Executive Vice President, People, Reconciliation, ~~Strategy~~ & Transformation Division	Realization and support of Program vision and objectives
Executive Director, Information Systems & Technology	Strategic direction and oversight, financial support

Leadership Group	Support for Program objectives, DWI (SharePoint) projects and staff engagement/time investment
VP Leadership Committee (VLC)	Contract, funding review and approvals
Director, Architecture & Innovation / A&I SMEs, project support resources	DWI Strategic direction and oversight, Program/project guidance and technical support
DWI Steering Committee	Committee of program subject matter experts~~experts~~ to provide recommendations/input and enable project delivery (Leads: ED, IST and Director, A&I)
Director, Records & Information Services	DIM Program Strategic direction and oversight, project guidance
Manager, Digital Information (DIM Program Manager)	Program and project lead, project management, compliance review, user support, change management, Program efficacy, policies/processes, reporting, contract management
Program Business Analyst	Program technical requirements and tasks to support M365 and SharePoint projects, solution sustainment, compliance
Director, Cybersecurity	Security expertise and guidance
Director, IT / IT SMEs, project support resources	Technical expertise, ~~guidance~~guidance, and support
Director, IS	IS/BA technical support and expertise
Departmental Leads/Staff	DWI (SharePoint) project support and participation, adherence to meeting schedules, ~~tasks~~tasks, and timelines

Program Contributors – Contractors

Contracted Contributor	Program Contribution / Value
Gravity Union – Digital Transformation / ECM Consulting	Delivery of DWI projects (intranet rebuild and SharePoint site development). Transfer of knowledge and hands-on support to IST staff who will become accountable for maintaining and sustaining the "workplace" upon contract completion.
File IT Solutions – Records & Information Management Consulting	Facilitation and delivery of SharePoint prerequisite work through departmental shared drive records classification, ~~organization~~organization, and de-duplication – focus on alignment/compliance with Commission records policy framework. Day-to-day project management and support provided by Manager, Digital Information.

Commented [AD12]: This needs to be updated to current contractor.

Program Roles & Responsibilities

	Executive Program Champion -Ines Piccinino	DWI Steering Committee	Program Sponsor – Ab Dosil	DWI Program Director (Architecture & Innovation) – Derek Mathews	RM Program Director (Records & Info Services) – Kathryn Smerechinskiy	**DIM Program Manager – Mahia Frost**	Program Business Analyst – 2022/23 Business Planning	IST Program/Project Resources – As Assigned	Departments - Site Owners and Users	Contracted Service Providers – Gravity Union	Contracted Service Providers – File IT Solutions
Program vision, establishing Executive buy-in of Program value	AR		C	I	I	I					
Program vision, Championing amongst Leadership Group, Executive liaison, VLC liaison	I		AR	C	C	C					
Ensuring alignment to Strategic & Capital plans	I		AR	C	C	C				C	
Program leadership and planning to achieve vision & objectives	I		C	A	A	R				C	
DWI contract & budget management, reporting	I	I	A	AR	I	I				C	
Hiring and/or allocation of Program resources	I		C	AR	AR	R		I			
Project planning & management, reporting		I	I	A	A	R		I	I	C	C
RM contract & budget management, reporting			I	I	A	R					C
Contractor liaison			AR	AR	AR	AR				R	R
Project championing, communications, change management	I	I	C	C	C	R	R	I		C	C
Project task execution & delivery, RM subject matter expertise, M365 IT technical expertise		I	A	A	A	AR	R	C	I	C	C
Solution sustainment, subject matter expertise, user training, ~~supporting~~supporting, and reinforcing change	I	I	A	A	AR	AR	R	C	I	C	C
Compliance with legislated requirements & processes, auditing		I	A	A	AR	AR	R	C	I	AR	AR

Section 13

Approval

This charter formally authorizes the new Digital Information Management (DIM) Program, based on the information outlined in this charter.

Approved by:

Approval Date:

Revision History

Version	Description of updates
0.1	Consolidation of program concept into Program Charter
0.2	

BRITISH COLUMBIA ENERGY REGULATOR

General Service Agreement

For Administration Purpose Only

Account No: 55510-215-000002 **Solicitation No: Quoted**

Contract No: 21524001

BETWEEN	AND
British Columbia Energy Regulator also referred to as "Regulator"	**FY Information Management Consulting also referred to as the "Contractor"**
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	8508 Betts Road Wardner, BC V0B 2J0
Phone number: 250.419.4400 **Email:** procurement@bc-er.ca	**Phone Number: 250.417.1229** **Email:** michelle@fyinformation.ca

THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS AND CONDITIONS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: Electronic Filing Structure Consultant (See Attached)

Term: Start Date: September 1, 2023 **End Date**: March 31, 2024

SCHEDULE B - FEES AND EXPENSES:	
Fees: $ 25,000	Expenses: $
Billing Date(s): **Monthly / Upon Invoice**	Maximum Amount: **$ 25,000**

SCHEDULE C - APPROVED SUBCONTRACTOR(S):
N/A

SCHEDULE D - INSURANCE:
(See Attached)

SCHEDULE E – PRIVACY PROTECTION:
(See Attached)

SCHEDULE F – ADDITIONAL TERMS:
N/A

SCHEDULE G – SECURITY:
N/A

SIGNED AND DELIVERED on the 6th day of September 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 1st day of September 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature	Signature
Mahia Frost	**Michelle Barroca**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF GENERAL SERVICE AGREEMENT

1 DEFINITIONS

General

In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
(b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
(c) "Material" means the Produced Material and the Received Material;
(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;
(f) "Services" means the services described in Schedule A;
(g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
(h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by the Regulator

2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

Confirmation of non-written instructions

2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set forth in Schedule B:

(a) The fees described in that Schedule, and
(b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's judgment, are necessarily incurred by the Contractor in providing the Services.
(c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

Appropriation

3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must apply for and, immediately on receipt, remit to the Regulator any available refund, rebate or remission of federal or provincial tax or duty that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

4 REPRESENTATIONS AND WARRANTIES

4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,

(a) All information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
(b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services, and
(c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

(d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and

(e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

(a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and

(b) Comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:

(a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;

(b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or

(c) If it is information in any Incorporated Material.

Public announcements

5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

5.5 The Contractor must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

Ownership and delivery of Material

6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

Matters respecting intellectual property

6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:

(a) Received Material that the Contractor receives from the Regulator; and

(b) Produced Material, other than any Incorporated Material.

Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:

(a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and

(b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

7 RECORDS AND REPORTS

Work reporting

7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

8 AUDIT

8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Regulator and the Regulator's employees and agents.

Insurance

9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

Workers compensation

9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:

(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and

(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

9.5 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

(a) "Event of Force Majeure" means one the following events:

(i) a natural disaster, fire, flood, storm, epidemic or power failure,

(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and

(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

(a) "Event of Default" means any of the following:
  (i) an Insolvency Event,
  (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
  (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:
  (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
  (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
  (iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
  (iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
  (v) the Contractor ceases, in the Regulator's reasonable opinion, to carry on business as a going concern.

Regulator's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Regulator may, at its option, elect to do any one or more of the following:
(a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
(b) Pursue any remedy or take any other action available to it at law or in equity; or
(c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Regulator to exercise its rights in relation to an Event of Default will constitute a waiver by the Regulator of such rights.

Regulator's right to terminate other than for default

11.4 In addition to the Regulator's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Regulator may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Regulator terminates this Agreement under section 11.4:
(a) The Regulator must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Regulator's satisfaction before termination of this Agreement; and
(b) The Contractor must, within 30 days of such termination, repay to the Regulator any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Regulator has notified the Contractor in writing was not completed to the Regulator's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Regulator of the amount described in section 11.5(a) discharges the Regulator from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Regulator of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
(a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
(b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
(c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
(a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
(b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
(c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email address

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Regulator's prior written consent.

Subcontracting

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Regulator's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
(a) Any person retained by the Contractor to perform obligations under this Agreement; and
(b) Any person retained by a person described in paragraph (a) to perform those obligations.
(c) Fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
(a) An employee or partner of the Regulator; or
(b) An agent of the Regulator except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Regulator

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:
(a) …"Includes" and "including" are not intended to be limiting;
(b) …Unless the context otherwise requires, references to sections by number are to sections of this Agreement;
(c) … The Contractor and the Regulator are referred to as "the parties" and each of them as a "party";
(d) …"Attached" means attached to this Agreement when used in relation to a schedule;
(e) … Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
(f) … The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
(g) …"Person" includes an individual, partnership, corporation or legal entity of any nature; and
(h) … Unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE A
SERVICES

This Schedule forms part of the agreement

Contract No: 21524001

DESCRIPTION OF SERVICES

The Contractor will assist Regulator staff in the formation of folder structures and folder naming conventions for one branch with 4 departments, containing roughly 270,000 documents.

Using established project framework from previous shared drive organization projects as a foundation, the Contractor will be:

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions, when appropriate
- Moving folders and associated records to the new folder structure (with user acceptance/permission); outside of business hours when required, to avoid disruption to information access
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

The Contractor will provide user support, training and change management by:

- Effectively initiating electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training to staff on the use and maintenance of the new shared drive folder structure

Reporting Requirements

- The Contractor will provide briefings, status updates/reports, and final results reports as requested
- The Contractor will maintain a current work plan and project schedule and provide updates as needed.

TERMS

The term of this Agreement commences on September 1, 2023 and ends on March 31, 2024.

KEY PERSONNEL

All notice to the Regulator will be sent to the Contract Manager:

Mahia Frost
Director, Records and Information Services
Mahia.Frost@bc-er.ca

Contractor Initials: _____ BC Energy Regulator (authorized initials): CCMFMF

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement.

Contract No: 21524001

1. Fees will be paid at an hourly rate of $135 per hour for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, $25,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is $25,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: _____ BC Energy Regulator (authorized initials): CMF

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE D
Insurance

This Schedule forms part of the agreement.

Contract No: 21524001

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
   (a) Commercial General Liability in an amount not less than **$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Regulator as an additional insured,
      (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause;

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Regulator.

3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: _____ BC Energy Regulator (authorized initials): CMF

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21524001

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: _____ BC Energy Regulator (authorized initials): CMF

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21524001

Storage and access to personal information

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the Commissioner under the Act; and
    (b) any direction given by the Regulator under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the Commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: _____ BC Energy Regulator (authorized initials): CMF

BRITISH COLUMBIA ENERGY REGULATOR

General Service Agreement

For Administration Purpose Only

Account No: 55510-215-000002 **Solicitation No: Quoted**

Contract No: 21525001

BETWEEN	AND
British Columbia Energy Regulator also referred to as "Regulator"	**FY Information Management Consulting also referred to as the "Contractor"**
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	8508 Betts Road Wardner, BC V0B 2J0
Phone number: 250.419.4400 **Email:** procurement@bc-er.ca	**Phone Number: 250.417.1229** **Email:** michelle@fyinformation.ca

THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS AND CONDITIONS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: Electronic Filing Structure Consultant (See Attached)

Term: Start Date: April 1, 2024 **End Date**: March 31, 2025

SCHEDULE B - FEES AND EXPENSES:	
Fees: $ 75,000	Expenses: $
Billing Date(s): **Monthly / Upon Invoice**	Maximum Amount: **$ 75,000**

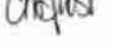
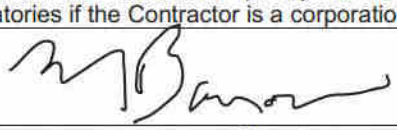
SCHEDULE C - APPROVED SUBCONTRACTOR(S):
N/A

SCHEDULE D - INSURANCE:
(See Attached)

SCHEDULE E – PRIVACY PROTECTION:
(See Attached)

SCHEDULE F – ADDITIONAL TERMS:
N/A

SCHEDULE G – SECURITY:
N/A

SIGNED AND DELIVERED on the 2nd day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 2nd day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
Mahia Frost	**Michelle Barroca**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF GENERAL SERVICE AGREEMENT

1 DEFINITIONS

General

In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
(b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
(c) "Material" means the Produced Material and the Received Material;
(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;
(f) "Services" means the services described in Schedule A;
(g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
(h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by the Regulator

2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

Confirmation of non-written instructions

2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set forth in Schedule B:

(a) The fees described in that Schedule, and
(b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's judgment, are necessarily incurred by the Contractor in providing the Services.
(c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

Appropriation

3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must apply for and, immediately on receipt, remit to the Regulator any available refund, rebate or remission of federal or provincial tax or duty that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

4 REPRESENTATIONS AND WARRANTIES

4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,

(a) All information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
(b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services, and
(c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

(d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and

(e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:
(a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and
(b) Comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:
(a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
(b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or
(c) If it is information in any Incorporated Material.

Public announcements

5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

5.5 The Contractor must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

Ownership and delivery of Material

6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

Matters respecting intellectual property

6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:
(a) Received Material that the Contractor receives from the Regulator; and
(b) Produced Material, other than any Incorporated Material.
Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:
(a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and
(b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

7 RECORDS AND REPORTS

Work reporting

7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

8 AUDIT

8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Regulator and the Regulator's employees and agents.

Insurance

9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

Workers compensation

9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

9.5 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:
(a) "Event of Force Majeure" means one the following events:
(i) a natural disaster, fire, flood, storm, epidemic or power failure,
(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

(a) "Event of Default" means any of the following:
  (i) an Insolvency Event,
  (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
  (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:
  (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
  (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
  (iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
  (iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
  (v) the Contractor ceases, in the Regulator's reasonable opinion, to carry on business as a going concern.

Regulator's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Regulator may, at its option, elect to do any one or more of the following:
(a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
(b) Pursue any remedy or take any other action available to it at law or in equity; or
(c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Regulator to exercise its rights in relation to an Event of Default will constitute a waiver by the Regulator of such rights.

Regulator's right to terminate other than for default

11.4 In addition to the Regulator's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Regulator may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Regulator terminates this Agreement under section 11.4:
(a) The Regulator must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Regulator's satisfaction before termination of this Agreement; and
(b) The Contractor must, within 30 days of such termination, repay to the Regulator any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Regulator has notified the Contractor in writing was not completed to the Regulator's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Regulator of the amount described in section 11.5(a) discharges the Regulator from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Regulator of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
(a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
(b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
(c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
(a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
(b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
(c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email address

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Regulator's prior written consent.

Subcontracting

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Regulator's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
(a) Any person retained by the Contractor to perform obligations under this Agreement; and
(b) Any person retained by a person described in paragraph (a) to perform those obligations.
(c) Fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
(a) An employee or partner of the Regulator; or
(b) An agent of the Regulator except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Regulator

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:
(a) …"Includes" and "including" are not intended to be limiting;
(b) …Unless the context otherwise requires, references to sections by number are to sections of this Agreement;
(c) … The Contractor and the Regulator are referred to as "the parties" and each of them as a "party";
(d) …"Attached" means attached to this Agreement when used in relation to a schedule;
(e) … Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
(f) … The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
(g) …"Person" includes an individual, partnership, corporation or legal entity of any nature; and
(h) … Unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE A
SERVICES

This Schedule forms part of the agreement

Contract No: 21525001

DESCRIPTION OF SERVICES

The Contractor will assist Regulator staff in the formation of centralized shared drive folder structures which align to Regulator standards.

Using established project framework from previous shared drive organization projects as a foundation, the Contractor will be:

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions, when appropriate
- Moving folders and associated records to the new folder structure (with user acceptance/permission); outside of business hours when required to avoid disruption to information access
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition and readying them for disposition by centralizing into one place
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

The Contractor will provide user support, training and change management by:

- Effectively initiating electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training to staff on the use and maintenance of the new shared drive folder structure

Reporting Requirements

- The Contractor will provide briefings, status updates/reports, and final results reports as requested
- The Contractor will maintain a current work plan and project schedule and provide updates as needed.

TERMS

The term of this Agreement commences on April 1, 2024 and ends on March 31, 2025. The Regulator, in its sole discretion, may renew this contract annually until March 31, 2027.

KEY PERSONNEL

All notice to the Regulator will be sent to the Contract Manager:

Mahia Frost
Director, Records and Information Services
Mahia.Frost@bc-er.ca

Contractor Initials: _____ BC Energy Regulator (authorized initials): _____

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement.

Contract No: 21525001

1. Fees will be paid at an hourly rate of $135 per hour for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, $75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is $75,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: _____ BC Energy Regulator (authorized initials): _____

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE D
Insurance

This Schedule forms part of the agreement.

Contract No: 21525001

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
   (a) Commercial General Liability in an amount not less than **$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Regulator as an additional insured,
      (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause;

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Regulator.

3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: _____ BC Energy Regulator (authorized initials): _____

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21525001

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: _____ BC Energy Regulator (authorized initials): _____

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21525001

Storage and access to personal information

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the Commissioner under the Act; and
    (b) any direction given by the Regulator under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the Commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: _____ BC Energy Regulator (authorized initials): _____

BC Oil & Gas COMMISSION

General Service Agreement

For Administration Purpose Only

Account No:55510-251-000003

Solicitation No: 25120001

Contract No: 25122001

BETWEEN	AND
Oil and Gas Commission **also referred to as "Commission"**	**File IT Solutions** **also referred to as the "Contractor"**
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	810 Shamrock Street Victoria, BC V8X 2V1
Phone number: 250.419.4487 **Email:** Kathryn.Smerechinskiy@bcogc.ca	**Phone Number:** 250.386.3487 **Email:** Laurie.Phillips@fileitsolutions.com

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: ARCS / ORCS Filing Structure Development (See attached)

Term: Start Date: April 19, 2021 **End Date**: March 31, 2022

SCHEDULE B - FEES AND EXPENSES:	
Fees: **$ 55 per hour**	Expenses: $ N/A
Billing Date(s): **Upon Invoice**	Maximum Amount: **$ 75,000**

SCHEDULE C - APPROVED SUBCONTRACTOR(S): See attached.

SCHEDULE D - INSURANCE: See attached.

SCHEDULE E – PRIVACY PROTECTION: See attached.

SCHEDULE F – ADDITIONAL TERMS: N/A

SCHEDULE G – SECURITY: See attached.

SIGNED AND DELIVERED on the 25th day of March 2021 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 25th day of March 2021 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
K. Smerechinskiy	Laurie Phillips
Signature	Signature
Kathryn Smerechinskiy	**Laurie Phillips**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF GENERAL SERVICE AGREEMENT

1 DEFINITIONS

General

In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
(b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
(c) "Material" means the Produced Material and the Received Material;
(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;
(f) "Services" means the services described in Schedule A;
(g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
(h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Commission

2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

Confirmation of non-written instructions

2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set forth in Schedule B:

(a) The fees described in that Schedule, and
(b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Commission's judgment, are necessarily incurred by the Contractor in providing the Services.
(c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

Appropriation

3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must apply for and, immediately on receipt, remit to the Commission any available refund, rebate or remission of federal or provincial tax or duty that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

4 REPRESENTATIONS AND WARRANTIES

4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,

(a) All information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct.
(b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services; and
(c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

(d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor; and

(e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

(a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and

(b) Comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:

(a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;

(b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or

(c) If it is information in any Incorporated Material.

Public announcements

5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

5.5 The Contractor must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

Ownership and delivery of Material

6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

Matters respecting intellectual property

6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:

(a) Received Material that the Contractor receives from the Commission; and

(b) Produced Material, other than any Incorporated Material.

Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:

(a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and

(b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

7 RECORDS AND REPORTS

Work reporting

7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

8 AUDIT

8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material, and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Commission and the Commission's employees and agents.

Insurance

9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

Workers compensation

9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:

(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and

(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

9.5 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

(a) "Event of Force Majeure" means one the following events:

(i) a natural disaster, fire, flood, storm, epidemic or power failure,

(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and

(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

(a) "Event of Default" means any of the following:
(i) an Insolvency Event,
(ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
(iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:
(i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
(ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
(iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
(iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
(v) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

Commission's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:
(a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
(b) Pursue any remedy or take any other action available to it at law or in equity; or
(c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

Commission's right to terminate other than for default

11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:
(a) The Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and
(b) The Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
(a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
(b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
(c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
(a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
(b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
(c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email address

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Commission's prior written consent.

Subcontracting

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
(a) Any person retained by the Contractor to perform obligations under this Agreement; and
(b) Any person retained by a person described in paragraph (a) to perform those obligations,
fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
(a) An employee or partner of the Commission; or
(b) An agent of the Commission except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Commission

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Commission.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Commission otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Commission must make available to the Contractor all information in the Commission's possession which the Commission considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Commission's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Commission under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Commission or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Commission or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:
(a) "includes" and "including" are not intended to be limiting;
(b) Unless the context otherwise requires, references to sections by number are to sections of this Agreement;
(c) The Contractor and the Commission are referred to as "the parties" and each of them as a "party";
(d) "Attached" means attached to this Agreement when used in relation to a schedule;
(e) Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
(f) The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
(g) "Person" includes an individual, partnership, corporation or legal entity of any nature; and
(h) Unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

BC Oil & Gas COMMISSION

SCHEDULE A
SERVICES

This Schedule forms part of the agreement

Contract No: 25122001

The Contractor will provide the following services:

DESCRIPTION OF SERVICES

Outputs / Outcomes

Establishment of folder structures and folder naming conventions

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions
- Moving folders and associated records to the new folder structure (with user acceptance/permission)
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

User support, training and change management:

- Effectively initiating each electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training (formal or desk-side) to staff on the use and maintenance of the new shared drive folder structure

Reporting Requirements

- Providing briefings, status updates/reports, and final results reports as requested
- Maintaining statistics/metrics for project tracking and communication purposes
- Maintaining a current work plan and project schedule

TERMS

The term of this Agreement commences on April 19, 2021 and ends on March 31, 2022.

KEY PERSONNEL

All notice to the Commission will be sent to the Contract Manager:

Kathryn Smerechinskiy
2950 Jutland Road
Victoria, BC V8T 5K2
250-419-4487

The Key Personnel of the Contractor are as follows:

(a) Marion Villines

BC Oil & Gas COMMISSION

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement

Contract No: 25122001

1. Fees will be paid at an hourly/daily rate of: $55 per hour/day (8 hrs = 1 day), for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, $75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

2. The Contractor should submit to the Commission, upon completion of the project, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is $75,000 plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: _____ Oil and Gas Commission (authorized initials): _____

BC Oil & Gas COMMISSION

SCHEDULE C
Approved Sub-contractor

This Schedule forms part of the agreement	**Contract No: 25122001**

The following sub-contractor(s) has been approved under this Agreement:

1. Marion Villines

BC Oil & Gas COMMISSION

SCHEDULE D
Insurance

This Schedule forms part of the agreement

Contract No: 25122001

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
   (a) Commercial General Liability in an amount not less than **$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Commission as an additional insured,
      (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause.

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Commission.

3. The Contractor must provide the Commission with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: _____ Oil and Gas Commission (authorized initials): _____

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials: _____ Oil and Gas Commission (authorized initials) _____

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Commission under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Definitions

BC Oil & Gas COMMISSION

SCHEDULE G
Security

This Schedule forms part of the agreement.

Contract No: 25122001

1. In this Schedule,
   a. "Equipment" means any equipment, including interconnected systems or subsystems of equipment, software and networks, used or to be used by the Contractor to provide the Services;
   b. "Facilities" means any facilities at which the Contractor provides or is to provide the Services;
   c. "Information" means information
      i. in the Material, or
      ii. accessed, produced or obtained by the Contractor (whether verbally, electronically or otherwise) as a result of the Agreement;
   d. "Record" means a "record" as defined in the Interpretation Act;
   e. "Sensitive Information" means
      i. Information that is "personal information" as defined in the Freedom of Information and Protection of Privacy Act, or
      ii. any other Information specified as "Sensitive Information" in Appendix G6, if attached; and
   f. "Services Worker" means an individual involved in providing the Services for or on behalf of the Contractor and, for greater certainty, may include
      i. the Contractor or a subcontractor if an individual, or
      ii. an employee or volunteer of the Contractor or of a subcontractor.

Schedule contains additional obligations

2. The obligations of the Contractor in this Schedule are in addition to any other obligations in the Agreement or the schedules attached to it relating to security including, without limitation, the obligations of the Contractor in the Privacy Protection Schedule, if attached.

Services Worker confidentiality agreements

3. The Contractor must not permit a Services Worker who is an employee or volunteer of the Contractor to have access to Sensitive Information unless the Services Worker has first entered into a confidentiality agreement with the Contractor to keep Sensitive Information confidential on substantially similar terms as those that apply to the Contractor under the Agreement.

Services Worker security screening

4. The Contractor may only permit a Services Worker who is an employee or a volunteer of the Contractor to have access to Sensitive Information or otherwise be involved in providing the Services if, after having subjected the Services Worker to the personnel security screening requirements and any additional requirements the Contractor may consider appropriate, the Contractor is satisfied that the Services Worker does not constitute an unreasonable security risk.

Services Worker activity logging

5. Subject to section 6, the Contractor must create and maintain detailed Records logging the activities of all Service Workers in relation to:
    a. their access to Sensitive Information; and
    b. other matters specified by the Commission in writing for the purposes of this section.
6. The Records described in section 5 must be made and maintained in a manner, and contain information, specified in Appendix G2, if attached.

Facilities and Equipment protection and access control

7. The Contractor must create, maintain and follow a documented process to:
    a. protect Facilities and Equipment of the Contractor required by the Contractor to provide the Services from loss, damage or any other occurrence that may result in any of those Facilities and Equipment being unavailable when required to provide the Services; and
    b. limit access to Facilities and Equipment of the Contractor
        i. being used by the Contractor to provide the Services, or
        ii. that may be used by someone to access Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons.

8. If the Commission makes available to the Contractor any Facilities or Equipment of the Commission for the use of the Contractor in providing the Services, the Contractor must comply with any policies and procedures provided to it by the Commission on acceptable use, protection of, and access to, such Facilities or Equipment.

Sensitive Information access control

9. The Contractor must:
    a. create, maintain and follow a documented process for limiting access to Sensitive Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons; and
    b. comply with the information access control requirements set out in Appendix G3, if attached.

Integrity of Information

10. The Contractor must:
    a. create, maintain and follow a documented process for maintaining the integrity of Information while possessed or accessed by the Contractor; and
    b. comply with the information integrity requirements set out in Appendix G4, if attached.

11. For the purposes of section 10, maintaining the integrity of Information means that, except to the extent expressly authorized by the Agreement or approved in writing by the Commission, the Information has:
    a. remained as complete as when it was acquired or accessed by the Contractor; and
    b. not been altered in any material respect.

Documentation of changes to processes

12. The Contractor must create and maintain detailed Records logging any changes it makes to the processes described in sections 7, 9 and 10.

Notice of security breaches

13. If Contractor becomes aware that:
    a. unauthorized access, collection, use, disclosure, alteration or disposal of Information or Records containing Information; or
    b. unauthorized access to Facilities or Equipment has occurred or is likely to occur (whether or not related to a failure by the Contractor to comply with this Schedule or the Agreement), the Contractor must immediately notify the Commission of the particulars of that occurrence or likely occurrence. If the Contractor provides a notification under this section other than in writing, that notification must be confirmed in writing to the Commission as soon as it is reasonably practicable for the Contractor to do so.

Review of security breaches

14. If the Commission decides to conduct a review of a matter described in section 13 (whether or not the matter came to the attention of the Commission as a result of a notification under section 13), the Contractor must, on the request of the Commission, participate in the review to the extent that it is reasonably practicable for the Contractor to do so.

Retention of Records

15. Unless the Agreement otherwise specifies, the Contractor must retain all Records in the Contractor's possession that contain Information until directed by the Commission in writing to dispose of them or deliver them as specified in the direction.

Storage of Records

16. Until disposed of or delivered in accordance with section 15, the Contractor must store any Records in the Contractor's possession that contain Information in accordance with the provisions of Appendix G5, if attached.

Audit

17. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy:
    a. any Records in the possession of the Contractor containing Information; or
    b. any of the Contractor's Information management policies or processes (including the processes described in sections 7, 9 and 10 and the logs described in sections 5 and 12) relevant to the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to the exercise by the Commission of the Commission's rights under this section.

Termination of Agreement

18. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

19. In this Schedule, unless otherwise specified:
    a. references to sections are to sections of this Schedule; and
    b. references to appendices are to the appendices attached to this Schedule.

20. Any reference to the "Contractor" in this Schedule includes any subcontractor retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors comply with this Schedule.

21. The appendices attached to this Schedule are part of this Schedule.

22. If there is a conflict between a provision in an appendix attached to this Schedule and any other provision of this Schedule, the provision in the appendix is inoperative to the extent of the conflict unless the appendix states that it operates despite a conflicting provision of this Schedule.

23. If there is a conflict between:

    a. a provision of the Agreement, this Schedule or an appendix attached to this Schedule; and
    b. a documented process required by this Schedule to be created or maintained by the Contractor

    the provision of the Agreement, Schedule or appendix will prevail to the extent of the conflict.

24. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

BC Oil & Gas COMMISSION

CONTRACT No. 25122001

CONTRACT AMENDMENT #2

THIS AMENDMENT MADE THIS 25th DAY OF MARCH 2022

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")
OF THE FIRST PART

AND:

FILE IT SOLUTIONS (HEREIN CALLED THE "CONTRACTOR")
OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into a General Services Agreement identified as Contract No. **25122001** (the "Agreement") for a term which initially commenced on April 19, 2021 and was scheduled to end on March 31, 2022;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment and renewal of the Agreement is made effective April 1, 2022.

2. The term of the contract is to be extended to March 2023. The term described in Schedule "A" is deleted and replaced with:

   The term of this Agreement commences on April 19, 2021 and is scheduled to end on March 31, 2023. The Commission has discretion to offer a one-year renewal of services at that time.

3. Maximum fees will increase by $75,000 from $75,000 to $150,000. Schedule B, Clauses 1 and 4 will be deleted and replace with:

   1. Fees will be paid at an hourly rate of: $55 per hour for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract and in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, $150,000, exclusive of any applicable taxes.

   6. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **$150,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

4. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 29 day of March 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 25 day of March 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
K. Smerechinskiy	Laurie Phillips
Signature	Signature
Kathryn Smerechinskiy	**Laurie Phillips**
Print Name	Print Name

BC Oil & Gas COMMISSION

General Service Agreement

For Administration Purpose Only

Account No:55510-251-000003

Solicitation No: 25120001

Contract No: 25122001

BETWEEN	AND
Oil and Gas Commission **also referred to as "Commission"**	**File IT Solutions** **also referred to as the "Contractor"**
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	810 Shamrock Street Victoria, BC V8X 2V1
Phone number: 250.419.4487 **Email:** Kathryn.Smerechinskiy@bcogc.ca	**Phone Number:** 250.386.3487 **Email:** Laurie.Phillips@fileitsolutions.com

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: ARCS / ORCS Filing Structure Development (See attached)

Term: Start Date: April 19, 2021 **End Date**: March 31, 2022

SCHEDULE B - FEES AND EXPENSES:	
Fees: **$ 55 per hour**	Expenses: $ N/A
Billing Date(s): **Upon Invoice**	Maximum Amount: **$ 75,000**

SCHEDULE C - APPROVED SUBCONTRACTOR(S): See attached.

SCHEDULE D - INSURANCE: See attached.

SCHEDULE E – PRIVACY PROTECTION: See attached.

SCHEDULE F – ADDITIONAL TERMS: N/A

SCHEDULE G – SECURITY: See attached.

SIGNED AND DELIVERED on the 25th day of March 2021 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 25th day of March 2021 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
K. Smerechinskiy	Laurie Phillips
Signature	Signature
Kathryn Smerechinskiy	**Laurie Phillips**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF GENERAL SERVICE AGREEMENT

1 DEFINITIONS

General

In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
(b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
(c) "Material" means the Produced Material and the Received Material;
(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;
(f) "Services" means the services described in Schedule A;
(g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
(h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Commission

2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

Confirmation of non-written instructions

2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set forth in Schedule B:

(a) The fees described in that Schedule, and
(b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Commission's judgment, are necessarily incurred by the Contractor in providing the Services.
(c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

Appropriation

3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must apply for and, immediately on receipt, remit to the Commission any available refund, rebate or remission of federal or provincial tax or duty that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

4 REPRESENTATIONS AND WARRANTIES

4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,

(a) All information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct.
(b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services, and
(c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

(d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor; and

(e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:

(a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and

(b) Comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:

(a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;

(b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or

(c) If it is information in any Incorporated Material.

Public announcements

5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

5.5 The Contractor must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

Ownership and delivery of Material

6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

Matters respecting intellectual property

6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:

(a) Received Material that the Contractor receives from the Commission; and

(b) Produced Material, other than any Incorporated Material.

Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:

(a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and

(b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

7 RECORDS AND REPORTS

Work reporting

7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

8 AUDIT

8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material, and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Commission and the Commission's employees and agents.

Insurance

9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

Workers compensation

9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:

(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and

(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

9.5 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.3 and 9.4.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

(a) "Event of Force Majeure" means one the following events:

(i) a natural disaster, fire, flood, storm, epidemic or power failure,

(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and

(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

(a) "Event of Default" means any of the following:
(i) an Insolvency Event,
(ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
(iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:
(i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
(ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
(iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
(iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
(v) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

Commission's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:
(a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
(b) Pursue any remedy or take any other action available to it at law or in equity; or
(c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

Commission's right to terminate other than for default

11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:
(a) The Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and
(b) The Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
(a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
(b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
(c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
(a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
(b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
(c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email address

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Commission's prior written consent.

Subcontracting

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
(a) Any person retained by the Contractor to perform obligations under this Agreement; and
(b) Any person retained by a person described in paragraph (a) to perform those obligations;
fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
(a) An employee or partner of the Commission; or
(b) An agent of the Commission except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Commission

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Commission.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Commission otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Commission must make available to the Contractor all information in the Commission's possession which the Commission considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Commission's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Commission under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Commission or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Commission or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:
(a) "includes" and "including" are not intended to be limiting;
(b) Unless the context otherwise requires, references to sections by number are to sections of this Agreement;
(c) The Contractor and the Commission are referred to as "the parties" and each of them as a "party";
(d) "Attached" means attached to this Agreement when used in relation to a schedule;
(e) Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
(f) The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
(g) "Person" includes an individual, partnership, corporation or legal entity of any nature; and
(h) Unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

BC Oil & Gas COMMISSION

SCHEDULE A
SERVICES

This Schedule forms part of the agreement

Contract No: 25122001

The Contractor will provide the following services:

DESCRIPTION OF SERVICES

Outputs / Outcomes

Establishment of folder structures and folder naming conventions

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions
- Moving folders and associated records to the new folder structure (with user acceptance/permission)
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

User support, training and change management:

- Effectively initiating each electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training (formal or desk-side) to staff on the use and maintenance of the new shared drive folder structure

Reporting Requirements

- Providing briefings, status updates/reports, and final results reports as requested
- Maintaining statistics/metrics for project tracking and communication purposes
- Maintaining a current work plan and project schedule

TERMS

The term of this Agreement commences on April 19, 2021 and ends on March 31, 2022.

KEY PERSONNEL

All notice to the Commission will be sent to the Contract Manager:

Kathryn Smerechinskiy
2950 Jutland Road
Victoria, BC V8T 5K2
250-419-4487

The Key Personnel of the Contractor are as follows:

(a) Marion Villines

BC Oil & Gas COMMISSION

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement

Contract No: 25122001

1. Fees will be paid at an hourly/daily rate of: $55 per hour/day (8 hrs = 1 day), for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, $75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

2. The Contractor should submit to the Commission, upon completion of the project, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is $75,000 plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: _____ Oil and Gas Commission (authorized initials): _____

BC Oil & Gas COMMISSION

SCHEDULE C
Approved Sub-contractor

This Schedule forms part of the agreement	**Contract No: 25122001**

The following sub-contractor(s) has been approved under this Agreement:

1. Marion Villines

Contractor Initials: _____ Oil and Gas Commission (authorized initials): _____

BC Oil & Gas COMMISSION

SCHEDULE D
Insurance

This Schedule forms part of the agreement

Contract No: 25122001

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
   (a) Commercial General Liability in an amount not less than **$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Commission as an additional insured,
      (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause.

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Commission.

3. The Contractor must provide the Commission with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: _____ Oil and Gas Commission (authorized initials): _____

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials: _____ Oil and Gas Commission (authorized initials) _____

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Commission under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Definitions

BC Oil & Gas COMMISSION

SCHEDULE G
Security

This Schedule forms part of the agreement.

Contract No: 25122001

1. In this Schedule,
   a. "Equipment" means any equipment, including interconnected systems or subsystems of equipment, software and networks, used or to be used by the Contractor to provide the Services;
   b. "Facilities" means any facilities at which the Contractor provides or is to provide the Services;
   c. "Information" means information
      i. in the Material, or
      ii. accessed, produced or obtained by the Contractor (whether verbally, electronically or otherwise) as a result of the Agreement;
   d. "Record" means a "record" as defined in the Interpretation Act;
   e. "Sensitive Information" means
      i. Information that is "personal information" as defined in the Freedom of Information and Protection of Privacy Act, or
      ii. any other Information specified as "Sensitive Information" in Appendix G6, if attached; and
   f. "Services Worker" means an individual involved in providing the Services for or on behalf of the Contractor and, for greater certainty, may include
      i. the Contractor or a subcontractor if an individual, or
      ii. an employee or volunteer of the Contractor or of a subcontractor.

Schedule contains additional obligations

2. The obligations of the Contractor in this Schedule are in addition to any other obligations in the Agreement or the schedules attached to it relating to security including, without limitation, the obligations of the Contractor in the Privacy Protection Schedule, if attached.

Services Worker confidentiality agreements

3. The Contractor must not permit a Services Worker who is an employee or volunteer of the Contractor to have access to Sensitive Information unless the Services Worker has first entered into a confidentiality agreement with the Contractor to keep Sensitive Information confidential on substantially similar terms as those that apply to the Contractor under the Agreement.

Services Worker security screening

4. The Contractor may only permit a Services Worker who is an employee or a volunteer of the Contractor to have access to Sensitive Information or otherwise be involved in providing the Services if, after having subjected the Services Worker to the personnel security screening requirements and any additional requirements the Contractor may consider appropriate, the Contractor is satisfied that the Services Worker does not constitute an unreasonable security risk.

Services Worker activity logging

5. Subject to section 6, the Contractor must create and maintain detailed Records logging the activities of all Service Workers in relation to:
    a. their access to Sensitive Information; and
    b. other matters specified by the Commission in writing for the purposes of this section.
6. The Records described in section 5 must be made and maintained in a manner, and contain information, specified in Appendix G2, if attached.

Facilities and Equipment protection and access control

7. The Contractor must create, maintain and follow a documented process to:
    a. protect Facilities and Equipment of the Contractor required by the Contractor to provide the Services from loss, damage or any other occurrence that may result in any of those Facilities and Equipment being unavailable when required to provide the Services; and
    b. limit access to Facilities and Equipment of the Contractor
        i. being used by the Contractor to provide the Services, or
        ii. that may be used by someone to access Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons.

8. If the Commission makes available to the Contractor any Facilities or Equipment of the Commission for the use of the Contractor in providing the Services, the Contractor must comply with any policies and procedures provided to it by the Commission on acceptable use, protection of, and access to, such Facilities or Equipment.

Sensitive Information access control

9. The Contractor must:
    a. create, maintain and follow a documented process for limiting access to Sensitive Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons; and
    b. comply with the information access control requirements set out in Appendix G3, if attached.

Integrity of Information

10. The Contractor must:
    a. create, maintain and follow a documented process for maintaining the integrity of Information while possessed or accessed by the Contractor; and
    b. comply with the information integrity requirements set out in Appendix G4, if attached.

11. For the purposes of section 10, maintaining the integrity of Information means that, except to the extent expressly authorized by the Agreement or approved in writing by the Commission, the Information has:
    a. remained as complete as when it was acquired or accessed by the Contractor; and
    b. not been altered in any material respect.

Documentation of changes to processes

12. The Contractor must create and maintain detailed Records logging any changes it makes to the processes described in sections 7, 9 and 10.

Notice of security breaches

13. If Contractor becomes aware that:
    a. unauthorized access, collection, use, disclosure, alteration or disposal of Information or Records containing Information; or
    b. unauthorized access to Facilities or Equipment has occurred or is likely to occur (whether or not related to a failure by the Contractor to comply with this Schedule or the Agreement), the Contractor must immediately notify the Commission of the particulars of that occurrence or likely occurrence. If the Contractor provides a notification under this section other than in writing, that notification must be confirmed in writing to the Commission as soon as it is reasonably practicable for the Contractor to do so.

Review of security breaches

14. If the Commission decides to conduct a review of a matter described in section 13 (whether or not the matter came to the attention of the Commission as a result of a notification under section 13), the Contractor must, on the request of the Commission, participate in the review to the extent that it is reasonably practicable for the Contractor to do so.

Retention of Records

15. Unless the Agreement otherwise specifies, the Contractor must retain all Records in the Contractor's possession that contain Information until directed by the Commission in writing to dispose of them or deliver them as specified in the direction.

Storage of Records

16. Until disposed of or delivered in accordance with section 15, the Contractor must store any Records in the Contractor's possession that contain Information in accordance with the provisions of Appendix G5, if attached.

Audit

17. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy:
    a. any Records in the possession of the Contractor containing Information; or
    b. any of the Contractor's Information management policies or processes (including the processes described in sections 7, 9 and 10 and the logs described in sections 5 and 12) relevant to the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to the exercise by the Commission of the Commission's rights under this section.

Termination of Agreement

18. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

19. In this Schedule, unless otherwise specified:
    a. references to sections are to sections of this Schedule; and
    b. references to appendices are to the appendices attached to this Schedule.

20. Any reference to the "Contractor" in this Schedule includes any subcontractor retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors comply with this Schedule.

21. The appendices attached to this Schedule are part of this Schedule.

22. If there is a conflict between a provision in an appendix attached to this Schedule and any other provision of this Schedule, the provision in the appendix is inoperative to the extent of the conflict unless the appendix states that it operates despite a conflicting provision of this Schedule.

23. If there is a conflict between:

    a. a provision of the Agreement, this Schedule or an appendix attached to this Schedule; and
    b. a documented process required by this Schedule to be created or maintained by the Contractor

    the provision of the Agreement, Schedule or appendix will prevail to the extent of the conflict.

24. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

BC Oil & Gas COMMISSION

CONTRACT No. 25122001

CONTRACT AMENDMENT #2

THIS AMENDMENT MADE THIS 25th DAY OF MARCH 2022

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")
OF THE FIRST PART

AND:

FILE IT SOLUTIONS (HEREIN CALLED THE "CONTRACTOR")
OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into a General Services Agreement identified as Contract No. **25122001** (the "Agreement") for a term which initially commenced on April 19, 2021 and was scheduled to end on March 31, 2022;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment and renewal of the Agreement is made effective April 1, 2022.

2. The term of the contract is to be extended to March 2023. The term described in Schedule "A" is deleted and replaced with:

   The term of this Agreement commences on April 19, 2021 and is scheduled to end on March 31, 2023. The Commission has discretion to offer a one-year renewal of services at that time.

3. Maximum fees will increase by $75,000 from $75,000 to $150,000. Schedule B, Clauses 1 and 4 will be deleted and replace with:

   1. Fees will be paid at an hourly rate of: $55 per hour for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract and in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, $150,000, exclusive of any applicable taxes.

   6. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **$150,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

4. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 29 day of March 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 25 day of March 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
K. Smerechinskiy	Laurie Phillips
Signature	Signature
Kathryn Smerechinskiy	**Laurie Phillips**
Print Name	Print Name

Information Technology Professional Service Agreement

For Administration Purpose Only

Account No: 15000-214-000005 **Solicitation No: RFP21422003**

Contract No: 21422002

BETWEEN	AND
Oil and Gas Commission **also referred to as the "Commission"**	**Gravity Union Solutions Limited** **also referred to as the "Contractor"**
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	1240 - 605 Robson Street Vancouver, BC V6B 5J3
Phone number: 250.419.4400 **Email:** procurement@bcogc.ca	**Phone Number: 604.782.1507** **Email:** mschweitzer@gravityunion.com

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: Development Services – Modern Digital Workplace (See attached)

Term: Start Date: February 1, 2022 **End Date**: March 31, 2024

SCHEDULE B - FEES AND EXPENSES:	
Fees: $ 200,000	Expenses: $
Billing Date(s): **Monthly / Upon Invoice**	Maximum Amount: **$ 200,000**

SCHEDULE C - APPROVED SUBCONTRACTOR(S):
N/A

SCHEDULE D - INSURANCE:
(See Attached)

SCHEDULE E – PRIVACY PROTECTION:
(See Attached)

SCHEDULE F – ADDITIONAL TERMS:
N/A

SCHEDULE G – SECURITY:
N/A

SIGNED AND DELIVERED on the 14th day of February 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 14 day of February 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature	Signature
Ab Dosil	**Michael Schweitzer**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

1 DEFINITIONS

General

1.1 In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;

(b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;

(c) "Material" means the Produced Material and the Received Material;

(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;

(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;

(f) "Services" means the services described in Part 2 of Schedule A;

(g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and

(h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill, and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Commission

2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions, but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

Confirmation of non-written instructions

2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set out in Schedule B:

(a) the fees described in that Schedule;

(b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Commission's opinion, are necessarily incurred by the Contractor in providing the Services; and

(c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b) .

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify in whole or in part the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

Appropriation

3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must:

(a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and

(b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Commission.

4 REPRESENTATIONS AND WARRANTIES

4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows:

(a) except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,

(i) all information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,

(ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and

(iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and

Contractor Initials: MS Oil and Gas Commission (authorized initials): _____

(b) if the Contractor is not an individual,
(i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
(ii) this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy
5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security
5.2 The Contractor must:
(a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:
(a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
(b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
(c) if it is information in any Incorporated Material.

Public announcements
5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion
5.5 The Contractor, must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material
6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

Ownership and delivery of Material
6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

Matters respecting intellectual property
6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:
(a) Received Material that the Contractor receives from the Commission; and
(b) Produced Material, other than any Incorporated Material.

Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material
6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:
(a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
(b) the right to sublicense or assign to third-parties any or all of the rights granted to the Commission under section 6.4(a).

Right of Commission to negotiate license of Produced Material
6.5 After the end of the Term, the Commission in its sole discretion, may negotiate with the Contractor to provide the Contractor a license (which may be exclusive or non-exclusive) for the Contractor to use, reproduce, modify or distribute some or all of the Produced Material.

7 RECORDS AND REPORTS

Work reporting
7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records
7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

8 AUDIT

8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity
9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by
(a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or

(b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

Monetary limitations of indemnity
9.2 The indemnification by the Contractor pursuant to section 9.1 is limited to:
(a) $2,000,000 per Loss; and
(b) $4,000,000 in the aggregate for all Losses.

Exceptions to monetary limitations
9.3 The limitations set out in section 9.2 do not apply to a Loss resulting from or relating to any of the following:
(a) bodily injury or damage to real property or tangible personal property;
(b) third-party intellectual property rights; or
(c) a breach of section 5.1, 5.2, 5.3 or 6.1 of this Agreement.

Commission to notify Contractor of Loss
9.4 To claim indemnification for a Loss pursuant to section 9.1, the Commission must notify the Contractor in writing of the Loss as soon as reasonably practicable after the Commission becomes aware of the Loss provided that a failure by the Commission to provide such notification will not invalidate the claim unless the Contractor is materially prejudiced by that failure.

Third-party intellectual property infringement claims
9.5 If the Loss is on the basis of a third-party claim that any element of the Material infringes the intellectual property rights of any person,
(a) then, without limiting section 9.1, the Contractor must defend the Commission against that claim at the Contractor's expense and the Contractor must pay all associated costs, damages and legal fees that a court or arbitrator finally awards or are included in a settlement agreed to by the Contractor; and
(b) the Commission must cooperate with the Contractor in the defence of the claim and, where appropriate in the discretion of the Commission, will allow the Contractor to appoint and instruct counsel and otherwise control the defence and any related settlement negotiations.

Insurance
9.6 The Contractor must comply with the Insurance Schedule attached as Schedule D.

Workers compensation
9.7 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Contractor Initials: MS Oil and Gas Commission (authorized initials): _____

Personal optional protection

9.8 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:

(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and

(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage

9.9 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.7 and 9.8.

10 FORCE MAJEURE

Definitions relating to force majeure

10.1 In this section and sections 10.2 and 10.3:

(a) "Event of Force Majeure" means one of the following events:

(i) a natural disaster, fire, flood, storm, epidemic or power failure,

(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,

(iii) a strike (including illegal work stoppage or slowdown) or lockout, or

(iv) a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and

(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:

(a) "Event of Default" means any of the following:

(i) an Insolvency Event,

(ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or

(iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:

(i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,

(ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency,

(iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,

(iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),

(v) a receiver or receiver-manager is appointed for any of the Contractor's property, or

(vi) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

Commission's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:

(a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;

(b) pursue any remedy or take any other action available to it at law or in equity; or

(c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

Commission's right to terminate other than for default

11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:

(a) the Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and

(b) the Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:

(a) the parties must initially attempt to resolve the dispute through collaborative negotiation;

(b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and

(c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of arbitration or mediation

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a arbitration or mediation under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:

(a) by email to the addressee's email specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;

(b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or

(c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email

13.2 Either party may from time to time give notice to the other party of a substitute address or email, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email specified for the party giving the notice.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

Assignment

13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Commission's prior written consent. Upon providing written notice to the Contractor, the Commission may assign to any person any of the Commission's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Commission's obligations under this Agreement

Subcontracting

13.4. The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:

(a) any person retained by the Contractor to perform obligations under this Agreement; and

(b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.5, 7.1, 7.2, 8.1, 9.1 to 9.6, 9.9, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:

(a) an employee or partner of the Commission; or

(b) an agent of the Commission except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Commission

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Commission.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Commission otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Commission must make available to the Contractor all information in the Commission's possession which the Commission considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Commission's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Commission under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:

(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and

(b) a provision in a schedule will prevail over any conflicting provision in a document attached to, or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Commission or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Commission or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:

(a) "includes" and "including" are not intended to be limiting;

(b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;

(c) the Contractor and the Commission are referred to as "the parties" and each of them as a "party";

(d) "attached" means attached to this Agreement when used in relation to a schedule;

(e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;

(f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;

(g) "person" includes an individual, partnership, corporation or legal entity of any nature; and

(h) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

SCHEDULE A
SERVICES

This Schedule forms part of the agreement.	Contract No: 21422002

Description of Services

The Contractor will provide services as proposed in December 2021 and as described below to architect and develop a high availability, collaborative and integrated digital workplace built on the M365 platform.

Services will include, but are not limited to the following as described in the original request:

- Project management services using industry best practices for iterative delivery
- Implementation of necessary M365 (and other integrated) services to deliver the scope, including
    - Technical analysis
    - UX and Design proposal
    - Development and implementation of sites and integrations
    - Testing and training technical staff
    - Migration to production
    - Ongoing go-live support
- Expert resources capable of ensuring the project meets objectives through effective and sustainable adoption of new tools
    - Stakeholder engagement and analysis
    - User experience considerations when designing services
    - Provide user training
    - Change management services to help effective adoption
    - Collaboration with Commission staff to transition to operations
    - Set up governance and document best practices
    - Security and privacy consultation when developing components of the digital workplace

The Commission will provide the following:
- Collaboration to ensure the project is aligned with intended objectives
- Business and technical product owners of various components of the digital workplace
- Access to business and technical SMEs, stakeholders, and sponsor
- Licensing and necessary access to Commission's M365 tenant
- Project champions to help mediate issues and resolve blockers

Outcomes

This initiative will be deemed successful when the following outcomes are realized. Based on staff interviews conducted during M365 evaluation, and in alignment with the Commission's Digital Workplace Program, this initiative aims to accomplish the following outcomes:

- Implement workplace tools that are user friendly and intuitive
- Ensure information is easily searchable and securely shareable
- Collaborate in real time, and remotely, in a digital environment
- Effectively manage asynchronous communication
- Socialize with other staff in a virtual environment using modern platforms
- Support communication and information access on the go securely (e.g., on mobile devices)
- Provide department ownership and control over their content
- Provide user process centric training to ensure effective adoption across staff with varied learning methods and demographics
- Ensure document libraries and migration of documents are aligned with the Commission's Electronic Document Retention and Management (EDRM) plan and recommendations
- Ensure a smooth process for complying with records management policies (e.g., applying document tags and retention policies)
- Apply governance structures that provide effective oversight to ensure a sustainable workplace implementation

Contractor Initials: MS Oil and Gas Commission (authorized initials):

Outcomes (Cont.)

- Supply a sustainable and scalable digital workplace architecture and processes to ensure effective ongoing operations
- Guarantee all services comply with the Freedom of Information and Protection of Privacy Act (FOIPPA), IT Infrastructure best practices, Commission's cybersecurity, and record management policies

The Commission expects the following to be part of the implementation:

- Technical and Logical SharePoint structure
  - The Commission is leaning towards a flat technical structure (i.e. not using subsites) to ensure ongoing flexibility
  - Sites can include employee facing sites (i.e. corporate), department sites (focused on individual departments), and project sites (focused on cross department teams)
- The logical structure (navigation, hierarchy, etc.) will be developed in parallel using the Navigation Mega Menu.

- Site Templates
  - Develop corporate branding across all pages
    - Common navigation
    - Common theme / colours
    - Unified search
    - Roll-up of News and Events
  - Develop standardized templates for (but not limited to)
    - Landing pages (department welcome pages, employee areas, etc.)
    - Logical subsites (e.g., department public and private pages, project pages)
    - Newsletters
    - News articles
- Multimedia management
  - Implement any multimedia file management tools (such as Streams) to enable easy and secure sharing of multimedia files, such as videos, images
- Document management and migration
  - Assist in migrating documents from shared drives and web servers to OneDrive or SharePoint
  - Assist in converting documents to site pages, where appropriate
  - Ensure records management policies are applied during migration
- Sustainable metadata usage
  - Work with the governance team to set up content within the term store
  - Ensure services implemented (e.g., document libraries) utilize meta data from the term store
  - Help develop policies for meta data usage and incorporate them into the centre of excellence
- Implement search refiners to ensure efficient and relevant content searching
- Collaboration
  - Review and refine the current Teams implementation to ensure effective use of Teams for collaboration and integration into other M365 services
- Socialization Platform
  - Implement a social media platform, such as Yammer, to enable non-business-related conversations
  - Assist in developing governance policies to ensure the platform follows Commission guidelines
- Sharing Corporate Information such as
  - News and Exec Updates
  - Internal staff updates (corporate and department level)
  - Newsletters (corporate and department level)
  - Appropriate combination of tools to publish and share content
- Adoption
  - User/Process centric training materials and adoption plan
  - Identify and develop training materials (including but not limited to recorded training sessions, manuals, short videos, new staff handbook, etc.)

Contractor Initials: MS Oil and Gas Commission (authorized initials):

  - Provide training to staff and other Commission trainers
  - Create a detailed plan and execute on change management activities
- Governance and Centre of Excellence
  - Help establish a sustainable centre of excellence and governance structure
  - Help establish a documentation hub for centre of excellence
  - Develop guidelines and best practices to sustainably maintain the centre of excellence
- Security
  - Defined security roles from M365 Global Administrators to End Users
  - A simple three-group security model for sites
    - Site Owners – Full Control
    - Site Members – Edit
    - Site Visitors – Read
  - Company-wide security groups
  - No external sharing of Commission information or data with the possible exception of project sites

The successful proponent is not expected to implement or re-implement:
- Any M365 services the Commission has already implemented, such as Teams
- Any setup of specific records management labels, classification, or policies

Reporting Requirements

Weekly a detailed status report will be delivered to BC Oil and Gas Commission's Project Manager. This report will contain at least the following information:

• Activities completed and progress against work plan(s) for the current week
• Issues requiring immediate attention by key personnel or impending deadlines for the project team's responsibilities (including projected impacts if deadlines are missed)
• Activities planned for the following week
• Running log of issues and risks
• Management of approvals and signoffs
• Financial summary

1. The Contractor agrees and confirms as follows:

a. All Contractor representatives, employees, sub-contractor representatives or sub-contractor employees attending a Commission office or field-based worksite at any time on or after January 10. 2022 will:
   i. be fully vaccinated against COVID-19 with a vaccine approved in Canada, including any available recommended booster doses; or
   ii. have received an exemption from the requirement to be fully vaccinated against COVID-19 from the Office of the Provincial Health Officer or for a valid reason under the BC Human Rights Code.

b. All Contractor representatives, employees, sub-contractor representatives or sub-contractor employees providing services relating to this Agreement will be provided with notice of the vaccination requirements identified in 1(a) prior to attending a Commission office of field-based worksite on or after January 10, 2022 and will be required to maintain proof of valid vaccination status.

c. The Contractor will obtain from each sub-contractor a true, accurate written certification of the sub-contractor's compliance with these vaccination requirements.

d. The Contractor agrees to provide the Commission with a true, accurate written certification of compliance with 1(a)-(c) at any time and agrees that such certification may be subject to verification by the Commission at any time.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

SCHEDULE A
SERVICES

This Schedule forms part of the agreement. | **Contract No: 21422002**

TERM

The term of this Agreement commences on February 1, 2022 and ends on March 31, 2024.

Work will be completed in 2 stages

Stage 1: Complete the scope of work including Digital Workplace foundations, implementation of the corporate portal, board portal, and initial department sites as prioritized with a total value up to $200,000.

Stage 2: On completion of stage one, an assessment will be completed to determine options for implementing stage two. Stage 2 will focus on additional Department, Team, and Project sites and may include overall improvements to the Digital Workplace implementation. Stage 2 will have a maximum value of $296,000 with work likely to begin in FY2023/24. This is subject to budget approval and the results and value realized from stage one of the project.

This is summarized in the following table

Stage	Phase	% Budget	Hours	Cost
1.	1. Foundation	12.5%	320	$61,950
	2. Corporate Portal	12.5%	320	$61,950
	3. Board Portal	6.25%	160	$30,975
	4. Initial Department Sites	8.75%	224	$45,125
	Sub Total	40%	1024	$200,000
2.	5. Departmental, Teams and Projects (160 hours per site)[1]	60%	1536	$296,600
	Total	100%	2560	$496,600

KEY PERSONNEL

All notices to the Commission will be sent to the Contract Manager:

Abhinav Rai
Manager, Business Intelligence, Research & Analytics
abhinav.rai@bcogc.ca

Derek Mathews
Director, Architecture & Innovation
derek.mathews@bcogc.ca

Invoices will be sent to:

Abhinav Rai
Manager, Business Intelligence, Research & Analytics
abhinav.rai@bcogc.ca

[1] Stage 2 above is dependent on the number of business units the Commission chooses to onboard into the new Digital Workplace portal.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

Derek Mathews
Director, Architecture & Innovation
derek.mathews@bcogc.ca

Lisa Gerlach
Manager, Communications
lisa.gerlach@bcogc.ca

Katie Cook
Information Systems & Technology Project Coordinator • Planning & Technology
katie.cook@bcogc.ca

The Key Personnel of the Contractor are as follows:

a. Michael Schweitzer | Vancouver, BC – CEO, Founder, and Lead Consultant
b. Kyal Creswell | Ottawa, Ont. – Solution Architect
c. Ellisa Kilmos | Vancouver, BC – Senior Consultant/UX Lead
d. Pauline Richer | Calgary, AB – M365 Consultant
e. Kelvin Yu | Vancouver, BC – M365 Consultant
f. Matt James | Calgary, AB – Senior Project Manager
g. Laura Bower | Vancouver, BC – Project Coordinator

BC Oil & Gas COMMISSION

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement. | **Contract No: 21422002**

1. Fees will be paid at an hourly rate as estimated and outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, $200,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Phase	% Budget	Hours	Cost
1 – Foundation	12.5%	320	$61,950
2 – Corporate and M365 Baseline Setup	12.5%	320	$61,950
3 – Departmental, Teams and Project Sites (12 department sites @ 160 hours per department site)	75%	1,920	$371,700
Total	100.0%	2,560	$496,600

Estimate By Role

Role	% Budget	Hours	Cost
Senior Project Manager	10.6%	271	$54,200
Lead Consultant	7%	180	$45,000
Senior Solution Architect	10.5%	270	$67,500
Senior Infrastructure Architect	11.1%	283	$56,600
Digital Transformation Analyst 1	30.4%	778	$136,150
Digital Transformation Analyst 2	30.4%	778	$136,150
Total	100.0%	2,560	$496,600

Role	Rate (per hour)
Senior Project Manager	$200
Lead Consultant	$250
Senior Solution Architect	$250
Senior Infrastructure Architect	$200
Digital Transformation Analyst	$175

Contractor Initials: MS Oil and Gas Commission (authorized initials):

2. The Contractor should submit to the Commission, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$200,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

SCHEDULE D
Insurance

This Schedule forms part of the agreement.	Contract No: 21422002

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
   (a) Commercial General Liability in an amount not less than **$2,000,000** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Commission as an additional insured,
      (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause;

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Commission.

3. The Contractor must provide the Commission with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Commission of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement. | **Contract No: 21422002**

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement. | **Contract No: 21422002**

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Commission under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: MS Oil and Gas Commission (authorized initials):

BC Oil & Gas COMMISSION

CONTRACT No. 21422002

CONTRACT AMENDMENT #1

THIS AMENDMENT MADE THIS 26th DAY OF SEPTEMBER 2022

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment is made effective October 1, 2022.
2. Maximum Fees will increase by $122,000 from $200,000 to $322,000. Clauses 1 and 4 will be removed and replaced with the following:
    1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **$322,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	$200
Lead Consultant	$250
Senior Solution Architect	$250
Senior Infrastructure Architect	$200
Digital Transformation Analyst	$175

BC Oil & Gas COMMISSION

CONTRACT No. 21422002

CONTRACT AMENDMENT #1

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$322,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 28th day of September 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 27 day of September 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	michael Schweitzer
Signature	Signature
Ab Dosil	**Michael Schweitzer**
Print Name	Print Name

BC Oil & Gas COMMISSION

CONTRACT No. 21422002

CONTRACT AMENDMENT #2

THIS AMENDMENT MADE THIS 2nd DAY OF FEBRUARY 2023

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment is made effective February 1, 2023.
2. Maximum Fees will increase by $38,000 from $322,000 to $360,000. Clauses 1 and 4 will be removed and replaced with the following:
    1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **$360,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	$200
Lead Consultant	$250
Senior Solution Architect	$250
Senior Infrastructure Architect	$200
Digital Transformation Analyst	$175

BC Oil & Gas COMMISSION

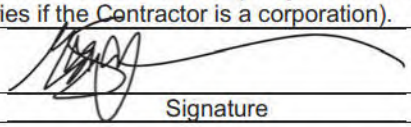
CONTRACT No. 21422002

CONTRACT AMENDMENT #2

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$360,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 07 day of February 2023 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the 07 day of February 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
Ab Dosil	**Michael Schweitzer**
Print Name	Print Name

BRITISH COLUMBIA ENERGY REGULATOR

CONTRACT No. 21422002

CONTRACT AMENDMENT #3

THIS AMENDMENT MADE THIS 8th DAY OF MAY 2023

BETWEEN:

BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment is made effective May 1, 2023.
2. Maximum Fees will increase by $200,000 from $360,000 to $560,000. Clauses 1 and 4 will be removed and replaced with the following:
    1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **$560,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	$200
Lead Consultant	$250
Senior Solution Architect	$250
Senior Infrastructure Architect	$200
Digital Transformation Analyst	$175

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$560,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

BRITISH COLUMBIA ENERGY REGULATOR

CONTRACT No. 21422002

CONTRACT AMENDMENT #3

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 11th day of May 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 10 day of May 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	michael Schweitzer
Signature	Signature
Ab Dosil	**Michael Schweitzer**
Print Name	Print Name

DocuSign Envelope ID: 5C475BF3-E267-46F5-91BF-58F87A0760B3

BRITISH COLUMBIA ENERGY REGULATOR

CONTRACT No. 21422002

CONTRACT AMENDMENT #4

THIS AMENDMENT MADE THIS 26th DAY OF APRIL 2024

BETWEEN:

BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into an Information Technology Professional Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022, and was scheduled to end on March 31, 2024;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment is made effective April 1, 2024.

2. The term of the Agreement is extended to March 31, 2025. The term described in Schedule "A" is deleted and replaced with:

   The term of this Agreement commences on February 1, 2022, and ends on March 31, 2025.

3. Maximum Fees will increase by $220,000 from $560,000 to $780,000. Clauses 1 and 4 will be removed and replaced with the following:

   1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **$780,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
Digital Transformation Analyst	$175 per hour
Solution and Infrastructure Architect	$200 per hour
Project Manager	$200 per hour

BRITISH COLUMBIA **ENERGY REGULATOR**

CONTRACT No. 21422002

CONTRACT AMENDMENT #4

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$780,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 29th day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 26 day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	DocuSigned by: D70CF583BAD6436...
Signature	Signature
Sara Dickinson	**Michael Schweitzer**
Print Name	Print Name

GRAVITY UNION

Department and Project Sites

BC Energy Regulator – Statement of Work

GRAVITY UNION

BC Energy Regulator — Department and Project Sites

Statement of Work

March 26, 2024

Confidentiality and Warranty

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Gravity Union Solution Limited.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, Gravity Union makes no representations and gives no warranties of whatever nature in respect of these documents, including and not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

Validity

This Statement of Work shall remain valid for 60 days.

Gold Certified Collabware Partner

Gold Microsoft Partner

Table of Contents

Introduction 3
Proposed Scope and Effort 3
Estimated Project Cost 4
Rates 4
Estimated Cost 4
Payments 4
Proposed Team 4
Assumptions 5
Support 5
Microsoft Gold Partner 5
Travel and Expenses 5
Cancellation 5
Change Orders 6
Payment 6
Authorization 6

Introduction

BC Energy Regulator engaged Gravity Union to design and configure SharePoint Online department and project sites for their organization. As the rollouts are still in progress, BCER requested Gravity Union to continue the rollout work of the SharePoint Departments, Teams, and Project sites and the related M365 infrastructure.

Proposed Scope and Effort

Gravity Union will design, configure, test and rollout nine additional department and project sites.

Based on the proposed effort and assumptions listed, below is the estimated cost.

Activity	Cost
Current state assessment, business requirements gathering, content discovery and audit, card sort exercise	
Iterative prototype build and test, solution refinements	
Migration planning and migration support	
End-user training, solution specific training, dry run of new solution, go-live support	
Retrospective and Transition to Operations	
Team meetings and check-ins for Digital Transformation Analyst and Solution Architect	
Project Management (at $200 per hour)	
Total	**$200,000**

Estimated Project Cost

Rates

Gravity Union's standard rates range between $175 and $250 per hour. Please see the rates table below for further details:

Activity and Role	Cost
Digital Transformation Analyst	$175 per hour
Solution and Infrastructure Architect	$200 per hour
Project Manager	$200 per hour

Estimated Cost

Gravity Union proposes a Time & Materials project budget targeting $200,000 +/- 25% where BC Energy Regulator is only billed for costs incurred, using the estimated costs below as our target budget. Any cost actuals beyond this budget would require prior approval before work execution or billing.

Payments

Invoices would be submitted at the end of each month, for hours worked during that month, due upon receipt.

Proposed Team

- Pauline Richer, Digital Transformation Analyst
- Denis Boico, Solution and Infrastructure Architect
- Thabata Granja, Project Manager
- Michael Schweitzer, Account Manager

Assumptions

- BCER will provide Gravity Union with relevant SharePoint account and access.
- The nine departments/groups will be determined. For this SOW, nine departments/groups are in scope.

Support

With resources across Canada, Gravity Union's standard support from 6:00am PT to 6:00 pm PT. Gravity Union can perform work outside of these hours when scheduled in advance and can negotiate support agreements for organizations beyond our regular hours on an as-needed basis.

Microsoft Gold Partner

As a Microsoft Gold Partner, we have access to resources and support directly from Microsoft to troubleshoot problems and issues and can escalate within Microsoft for support.

Travel and Expenses

At current, we do not anticipate any travel costs; however, travel costs and expenses will be itemized separately from hours for billing. There will be no mark-ups on travel costs and fees incurred.

Cancellation

The BC Energy Regulator is free to cancel this arrangement at any time. All time worked up to the notification of cancellation will be billed and owed to Gravity Union by BC Energy Regulator.

Change Orders

Proposed changes or extensions to the contracted work statement(s) must be in writing and approved by both BC Energy Regulator and Gravity Union before the commencement of work. Additional fees will be invoiced in the regular billing cycle described below.

Payment

The BC Energy Regulator will be billed at the end of each month for hours worked with payment due upon receipt. Included with each invoice will be a breakdown of hours with descriptions.

Authorization

By signing the below, all parties agree to enter into a contract for services as described in this document.

BC Energy Regulator

Name (printed) Derek Mathews Date March 28, 2024

Signature

Gravity Union Solutions Limited

Name (printed) Michael Schweitzer Date

Signature

BRITISH COLUMBIA ENERGY REGULATOR

Information Technology Professional Service Agreement

For Administration Purpose Only

Account No: 52050-214-000003 **Solicitation No: Quoted**

Contract No: 21424001

BETWEEN	AND
British Columbia Energy Regulator also referred to as "Regulator"	**Gravity Union Solutions Limited also referred to as the "Contractor"**
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	1240 - 605 Robson Street Vancouver, BC V6B 5J3
Phone number: 250.419.4400 **Email:** procurement@bc-er.ca	**Phone Number: 604.782.1507** **Email:** mschweitzer@gravityunion.com

THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

SCHEDULE A – list of Services: SharePoint Operational Portal Support Services (See attached)

Term: Start Date: May 1, 2023 **End Date**: March 31, 2024

SCHEDULE B - FEES AND EXPENSES:	
Fees: $ 50,000	Expenses: $
Billing Date(s): **Monthly / Upon Invoice**	Maximum Amount: **$ 50,000**

SCHEDULE C - APPROVED SUBCONTRACTOR(S):
N/A

SCHEDULE D - INSURANCE:
N/A

SCHEDULE E – PRIVACY PROTECTION:
N/A

SCHEDULE F – ADDITIONAL TERMS:
N/A

SCHEDULE G – SECURITY:
N/A

SIGNED AND DELIVERED on the 5th day of May 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 5th day of May 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature Signer ID: RAT24MNG10...	Signature
Derek Mathews	**Michael Schweitzer**
Print Name	Print Name

READ TERMS ON THE FOLLOWING PAGES

TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

1 DEFINITIONS

General

1.1 In this Agreement, unless the context otherwise requires:

(a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;

(b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;

(c) "Material" means the Produced Material and the Received Material;

(d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;

(e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;

(f) "Services" means the services described in Part 2 of Schedule A;

(g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and

(h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

Meaning of "record"

1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

2 SERVICES

Provision of services

2.1 The Contractor must provide the Services in accordance with this Agreement.

Term

2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

Supply of various items

2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

Standard of care

2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill, and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

Standards in relation to persons performing Services

2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

Instructions by Regulator

2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions, but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

Confirmation of non-written instructions

2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

Effectiveness of non-written instructions

2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

Applicable laws

2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

3 PAYMENT

Fees and expenses

3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set out in Schedule B:

(a) the fees described in that Schedule;

(b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's opinion, are necessarily incurred by the Contractor in providing the Services; and

(c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b) .

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

Statements of accounts

3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

Withholding of amounts

3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify in whole or in part the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

Appropriation

3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

Currency

3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

Non-resident income tax

3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

Prohibition against committing money

3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

Refunds of taxes

3.8 The Contractor must:

(a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and

(b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Regulator.

4 REPRESENTATIONS AND WARRANTIES

4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows:

(a) except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,

(i) all information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,

(ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and

(iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

(b) if the Contractor is not an individual,
  (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
  (ii) this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

5 PRIVACY, SECURITY AND CONFIDENTIALITY

Privacy

5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

Security

5.2 The Contractor must:
  (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and
  (b) comply with the Security Schedule attached as Schedule G.

Confidentiality

5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:
  (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
  (c) if it is information in any Incorporated Material.

Public announcements

5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

Restrictions on promotion

5.5 The Contractor, must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

6 MATERIAL AND INTELLECTUAL PROPERTY

Access to Material

6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

Ownership and delivery of Material

6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

Matters respecting intellectual property

6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:
  (a) Received Material that the Contractor receives from the Regulator; and
  (b) Produced Material, other than any Incorporated Material.

Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

Rights in relation to Incorporated Material

6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:
  (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
  (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Regulator under section 6.4(a).

Right of Regulator to negotiate license of Produced Material

6.5 After the end of the Term, the Regulator in its sole discretion, may negotiate with the Contractor to provide the Contractor a license (which may be exclusive or non-exclusive) for the Contractor to use, reproduce, modify or distribute some or all of the Produced Material.

7 RECORDS AND REPORTS

Work reporting

7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

Time and expense records

7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

8 AUDIT

8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

9 INDEMNITY AND INSURANCE

Indemnity

9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by
  (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
  (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

Monetary limitations of indemnity

9.2 The indemnification by the Contractor pursuant to section 9.1 is limited to:
  (a) $2,000,000 per Loss; and
  (b) $4,000,000 in the aggregate for all Losses.

Exceptions to monetary limitations

9.3 The limitations set out in section 9.2 do not apply to a Loss resulting from or relating to any of the following:
  (a) bodily injury or damage to real property or tangible personal property;
  (b) third-party intellectual property rights; or
  (c) a breach of section 5.1, 5.2, 5.3 or 6.1 of this Agreement.

Regulator to notify Contractor of Loss

9.4 To claim indemnification for a Loss pursuant to section 9.1, the Regulator must notify the Contractor in writing of the Loss as soon as reasonably practicable after the Regulator becomes aware of the Loss provided that a failure by the Regulator to provide such notification will not invalidate the claim unless the Contractor is materially prejudiced by that failure.

Third-party intellectual property infringement claims

9.5 If the Loss is on the basis of a third-party claim that any element of the Material infringes the intellectual property rights of any person,
  (a) then, without limiting section 9.1, the Contractor must defend the Regulator against that claim at the Contractor's expense and the Contractor must pay all associated costs, damages and legal fees that a court or arbitrator finally awards or are included in a settlement agreed to by the Contractor; and
  (b) the Regulator must cooperate with the Contractor in the defence of the claim and, where appropriate in the discretion of the Regulator, will allow the Contractor to appoint and instruct counsel and otherwise control the defence and any related settlement negotiations.

Insurance

9.6 The Contractor must comply with the Insurance Schedule attached as Schedule D.

Workers compensation

9.7 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Personal optional protection

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

9.8 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
(a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
(b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

Evidence of coverage
9.9 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.7 and 9.8.

10 FORCE MAJEURE

Definitions relating to force majeure
10.1 In this section and sections 10.2 and 10.3:
(a) "Event of Force Majeure" means one of the following events:
(i) a natural disaster, fire, flood, storm, epidemic or power failure,
(ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,
(iii) a strike (including illegal work stoppage or slowdown) or lockout, or
(iv) a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
(b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Consequence of Event of Force Majeure
10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party
10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

11 DEFAULT AND TERMINATION

Definitions relating to default and termination
11.1 In this section and sections 11.2 to 11.4:
(a) "Event of Default" means any of the following:
(i) an Insolvency Event,
(ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
(iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and

(b) "Insolvency Event" means any of the following:
(i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
(ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency,
(iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
(iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
(v) a receiver or receiver-manager is appointed for any of the Contractor's property, or
(vi) the Contractor ceases, in the Regulator's reasonable opinion, to carry on business as a going concern.

Regulator's options on default
11.2 On the happening of an Event of Default, or at any time thereafter, the Regulator may, at its option, elect to do any one or more of the following:
(a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
(b) pursue any remedy or take any other action available to it at law or in equity; or
(c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver
11.3 No failure or delay on the part of the Regulator to exercise its rights in relation to an Event of Default will constitute a waiver by the Regulator of such rights.

Regulator's right to terminate other than for default
11.4 In addition to the Regulator's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Regulator may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination
11.5 Unless Schedule B otherwise provides, if the Regulator terminates this Agreement under section 11.4:
(a) the Regulator must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Regulator's satisfaction before termination of this Agreement; and
(b) the Contractor must, within 30 days of such termination, repay to the Regulator any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Regulator has notified the Contractor in writing was not completed to the Regulator's satisfaction before termination of this Agreement.

Discharge of liability
11.6 The payment by the Regulator of the amount described in section 11.5(a) discharges the Regulator from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default
11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Regulator of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

12 DISPUTE RESOLUTION

Dispute resolution process
12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
(a) the parties must initially attempt to resolve the dispute through collaborative negotiation;
(b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
(c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

Location of arbitration or mediation
12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of arbitration or mediation
12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a arbitration or mediation under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

13 MISCELLANEOUS

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:

(a) by email to the addressee's email specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;

(b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or

(c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email

13.2 Either party may from time to time give notice to the other party of a substitute address or email, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Regulator's prior written consent. Upon providing written notice to the Contractor, the Regulator may assign to any person any of the Regulator's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Regulator's obligations under this Agreement

Subcontracting

13.4. The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Regulator's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:

(a) any person retained by the Contractor to perform obligations under this Agreement; and

(b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.5, 7.1, 7.2, 8.1, 9.1 to 9.6, 9.9, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:

(a) an employee or partner of the Regulator; or

(b) an agent of the Regulator except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

Personnel not to be employees of Regulator

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

Pertinent information

13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:

(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and

(b) a provision in a schedule will prevail over any conflicting provision in a document attached to, or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

14 INTERPRETATION

14.1 In this Agreement:

(a) "includes" and "including" are not intended to be limiting;

(b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;

(c) the Contractor and the Regulator are referred to as "the parties" and each of them as a "party";

(d) "attached" means attached to this Agreement when used in relation to a schedule;

(e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;

(f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;

(g) "person" includes an individual, partnership, corporation or legal entity of any nature; and

(h) unless the context otherwise requires, words expressed in the singular include the plural and *vice versa*.

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE A
SERVICES

This Schedule forms part of the agreement

Contract No: 21424001

DESCRIPTION OF SERVICES

The Contractor will provide operational support on an as-needed basis to support BCER's SharePoint Online portals and related M365 infrastructure. The Gravity Union Project Manager will triage support requests and delegate tasks accordingly to appropriate personnel (Analyst, Architect, Developer) assigned to the project.

TERM

The term of this Agreement commences on May 1, 2023 and ends on March 31, 2024. The Regulator may, in its sole discretion, renew this Agreement for up to two, one year terms.

INVOICES

All invoices to the Regulator will be sent to the following:

- Katie.Cook@bc-er.ca
- Derek.Mathews@bc-er.ca

KEY PERSONNEL

All notice to the Regulator will be sent to the Contract Manager:

Derek Mathews
Director, Architecture & Innovation
Derek.Mathews@bc-er.ca

The Key Personnel of the Contractor are as follows:

(a) Michael Schweitzer, Account Manager

(b) Thabata Granja, Project Manager

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE B
Fees and Expenses

This Schedule forms part of the agreement.

Contract No: 21424001

1. Fees will be paid at hourly rates as listed below, for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, $50,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	$200 per hour
Project Management services	$200 per hour

2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.

3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is $50,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE D
Insurance

This Schedule forms part of the agreement.

Contract No: 21424001

Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
   (a) Commercial General Liability in an amount not less than **$2,000,000** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
      (i) include the Regulator as an additional insured,
      (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
      (iii) include a cross liability clause;

2. All insurance described in section 1 of this Schedule must:
   (a) be primary; and
   (b) not require the sharing of any loss by any insurer of the Regulator.

3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
   (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
   (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Regulator of British Columbia Certificate of Insurance; and
   (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.

4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21424001

Definitions

1. In this Schedule,
   (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
   (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.

5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.

9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.

10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.

11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

BRITISH COLUMBIA ENERGY REGULATOR

SCHEDULE E
Privacy Protection

This Schedule forms part of the agreement.

Contract No: 21424001

Storage and access to personal information

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:
    (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
    (b) in accordance with section 13.

Disclosure of personal information

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Inspection of personal information

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
    (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
    (b) any direction given by the Regulator under this Schedule.

20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.

25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.

27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

DocuSign Envelope ID: 5C475BF3-E267-46F5-91BF-58F87A0760B3

BRITISH COLUMBIA ENERGY REGULATOR

CONTRACT No. 21424001

CONTRACT AMENDMENT #1

THIS AMENDMENT MADE THIS 26th DAY OF APRIL 2024

BETWEEN:

BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

A. The parties hereto entered into an Information Technology Professional Services Agreement identified as Contract No. 21424001 for a term which commenced on May 1, 2023, and was scheduled to end on March 31, 2024;

B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

1. This amendment is made effective April 1, 2024.

2. The term of the Agreement is extended to March 31, 2025. The term described in Schedule "A" is deleted and replaced with:

   The term of this Agreement commences on May 1, 2023, and ends on March 31, 2025. The Regulator may, in its sole discretion, renew this Agreement for one additional one-year term.

3. Maximum Fees will increase by $35,000 from $50,000 to $85,000. Clauses 1 and 4 will be removed and replaced with the following:

   1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **$85,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	$200 per hour
Project Management services	$200 per hour

BRITISH COLUMBIA **ENERGY REGULATOR**

CONTRACT No. 21424001

CONTRACT AMENDMENT #1

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **$85,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the 29th day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 26 day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature	Signature
Derek Mathews	**Michael Schweitzer**
Print Name	Print Name

GRAVITY UNION

Operational Support

BC Energy Regulator – Statement of Work

GRAVITY UNION

BC Energy Regulator — Operational Support

Statement of Work

March 26, 2024

Confidentiality and Warranty

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Gravity Union Solution Limited.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, Gravity Union makes no representations and gives no warranties of whatever nature in respect of these documents, including and not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

Validity

This Statement of Work shall remain valid for 60 days.

Gold Certified
Collabware Partner
collabware

Gold
Microsoft Partner
Microsoft

Table of Contents

Proposed Scope and Effort 3
Estimated Project Cost 3
Rates 3
Estimated Cost 3
Payments 4
Proposed Team 4
Assumptions 4
Support 4
Microsoft Gold Partner 4
Travel and Expenses 5
Cancellation 5
Change Orders 5
Payment 5
Authorization 6

Proposed Scope and Effort

The British Columbia Energy Regulator would like to continue engaging with Gravity Union to provide ongoing operational support on an as-needed basis to support their SharePoint Online portals and M365 Infrastructure support. The project budget is $50,000. The Gravity Union Project Manager will triage support requests and delegate tasks accordingly to the Analyst or Architect assigned to the project.

Estimated Project Cost

Rates

Gravity Union's standard rates range between $175 and $250 per hour. The Digital Transformation Analyst rate is $175 per hour, the Project Manager rate is $200 per hour, and the Senior Solution Architect rate is $250 per hour.

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	$200 per hour
Project Management services	$200 per hour

Estimated Cost

Gravity Union proposes a Time & Materials project budget targeting $50,000 where BC Energy Regulator is only billed for costs incurred, using the estimated costs below as our target budget. Any cost actuals beyond this budget would require prior approval before work execution or billing.

Payments

Invoices would be submitted at the end of each month, for hours worked during that month, due upon receipt.

Proposed Team

- Pauline Richer, Digital Transformation Analyst
- Denis Boico, Solution and Infrastructure Architect
- Thabata Granja, Project Manager
- Michael Schweitzer, Account Manager

Assumptions

- Gravity Union will have sufficient access to BCER's SharePoint solution.
- Requests from BCER will be sent to the Gravity Union Project Manager and triaged accordingly.

Support

With resources across Canada, Gravity Union's standard support from 6:00am PT to 6:00 pm PT. Gravity Union can perform work outside of these hours when scheduled in advance and can negotiate support agreements for organizations beyond our regular hours on an as-needed basis.

Microsoft Gold Partner

As a Microsoft Gold Partner, we have access to resources and support directly from Microsoft to troubleshoot problems and issues and can escalate within Microsoft for support.

Travel and Expenses

At current, we do not anticipate any travel costs; however, travel costs and expenses will be itemized separately from hours for billing. There will be no mark-ups on travel costs and fees incurred.

Cancellation

The BC Energy Regulator is free to cancel this arrangement at any time. All time worked up to the notification of cancellation will be billed and owed to Gravity Union by BC Energy Regulator.

Change Orders

Proposed changes or extensions to the contracted work statement(s) must be in writing and approved by both BC Energy Regulator and Gravity Union before the commencement of work. Additional fees will be invoiced in the regular billing cycle described below.

Payment

The BC Energy Regulator will be billed at the end of each month for hours worked with payment due upon receipt. Included with each invoice will be a breakdown of hours with descriptions.

Authorization

By signing the below, all parties agree to enter into a contract for services as described in this document.

BC Energy Regulator

Name (printed) Derek Mathews Date March 28, 2024

Signature

Gravity Union Solutions Limited

Name (printed) Michael Schweitzer Date _____

Signature _____

BRITISH COLUMBIA ENERGY REGULATOR

BC ENERGY REGULATOR
POSITION DESCRIPTION

POSITION TITLE:	Director, Records & Information Management	POSITION #:	573798
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Management Band B
Program Area:	Digital Transformation & Public Trust	LOCATION:	All BCER locations
SUPERVISOR'S TITLE:	Executive Director, Information Systems & Technology	POSITION #:	573019
SUPERVISOR'S CLASSIFICATION:	Management Band C	LOCATION:	Victoria

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation BCER's (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

JOB OVERVIEW

The Director, Records & Information Management (Director) oversees the BCER's records and information management, Freedom of Information (FOI) and privacy management programs. Reporting to the Executive Director, Information Systems & Technology, the Director is responsible for developing strategic goals and objectives and implementing strategies to advance the organization towards a state of maturity and legislative compliance in each area. A key requirement of the role involves establishing effective short and long-term solutions to content management, preservation, and governance in Microsoft Office 365 (M365) as the BCER's new digital platform. Other position accountabilities include leading multiple information, privacy and digital transformation projects and participating in corporate initiatives and committees as a subject matter expert.

ACCOUNTABILITIES

Leads, oversees, and manages the BCER's records and information (digital and physical) program in accordance with BC government legislation, directives, and standards:

- Provides strategic direction and advice to ensure the organization is fully compliant with all legislative information management requirements.
- Develops and implements strategies, policies, and processes to ensure compliant management and retention of content created and maintained in M365 applications (e.g., Teams, OneDrive and SharePoint) and BCER systems.

- Actively supports the planning, design, configuration and maintenance of M365 SharePoint sites as compliant records management/ECM solutions for BCER departments.
- Leads digital transformation and other related projects to improve access, preservation and ongoing management of BCER information.
- Supports organizational change management and facilitates employee training initiatives.
- Develops and implements information schedules to enable lifecycle management and disposition in accordance with the Information Management Act and related policies.
- Oversees corporate information disposition processes (digital and physical).
- Champions data stewardship and information governance practices.
- Implements client service delivery model improvements through policy, process and/or technological enhancements.
- Liaises with other government agencies on best practices and technological solutions.
- Collaborates with various departments and stakeholders, such as legal, Information Systems, Architecture and Innovation, and business units, to ensure alignment and integration of records and information management practices across the organization. Builds relationships and promotes a culture of cooperation and engagement.
- Assesses, supports the implementation, and maintaining of records management systems and technologies that enable efficient and secure management of records and information. This involves evaluating the organization's technological needs, selecting appropriate tools, and integrating them with existing systems.

Leads the administration and application of the Freedom of Information and Protection of Privacy Act (FOIPPA) across the organization:

- Oversees the administration of Freedom of Information (FOI) requests and proactive release of BCER information.
- Develops, implements, and maintains the BCER's Privacy Management Program as issued under FOIPPA s.36.2, including but not limited to oversight of breach response protocols and privacy impact assessments.
- Ensures information, policies and procedures related to FOI and privacy protection are readily available to BCER employees.
- Works collaboratively with employees, service providers, and other public bodies to build privacy protection into business activities involving the collection, use and/or disclosure of personal information.
- Prepares reports, briefing notes, and Estimates materials as required for supervisor and Executive.

Leads the Records and Information Services (RIS) Branch:

- Builds branch competencies, expertise, capacity, and overall organizational knowledge in relation to records and information management, Freedom of Information (FOI) and privacy.

ORGANIZATION CHART

Commissioner, Chief Executive Officer
Executive Vice President, People, Reconciliation & Transformation
Vice President, Digital Transformation & Public Trust
Executive Director, Information Systems & Technology
Director, Records & Information Management (TOPIC POSITION)

EDUCATION AND EXPERIENCE REQUIREMENTS

Education:

- Degree in Library and Information Studies, Information Management, Archival Studies, Business or Public Administration, or other related field, and a minimum of 7 years of professional information management experience in records and information management and information access in a provincial government setting, or an equivalent combination of education and minimum of 10 years related experience.

Experience:

- Demonstrated experience in a management role leading a records and information management program within a public sector setting.
- Experience leading new business development initiatives and/or digital transformation projects.

- Experience in supporting multiple clients in a diverse range of project portfolios, in a customer service environment.
- Demonstrated experience working in a project management and/or change management leadership role.
- Demonstrated experience supervising staff and/or contractors.
- Experience interpreting and applying BC legislation and government policies related to records and information management.
- Experience in developing and implementing records classification (information) schedules.
- Experience applying information lifecycle management and disposition processes (digital and physical records).
- Experience developing and delivering effective training to management and other levels of staff on information management requirements, principles and best practices.
- Strong working knowledge and understanding of electronic document and records management systems (EDRMS).
- Strong knowledge and experience using Microsoft Office 365 (M365) Teams, OneDrive and SharePoint and the application of records management functionality.
- Knowledge and experience in the application of the Freedom of Information and Protection of Privacy Act (FOIPPA) and Information Management Act (IMA).
- Experience reviewing and/or completing privacy impact assessments.
- Experience managing programs or providing specified knowledge in the area of natural resources, business management, or oil and gas industry operations.

FINANCIAL RESPONSIBILITES

- Responsible for the Records & Information Services Branch operational budget and capital costs associated with transformation initiatives.

KEY COMPETENCIES

Leadership - implies a desire to lead others, including diverse teams

Developing Others - involves a genuine intent to foster the long-term learning or development of others through coaching, managing performance and mentoring

Results Orientation - is a concern for surpassing a standard of excellence (striving for improvement, achievement, continuous improvement)

Managing Organization Resources - is the ability to understand and effectively manage organizational resources (e.g. people, materials, assets, budgets)

Teamwork and Cooperation - is the ability to work co-operatively within diverse teams, work groups and across the organization to achieve group and organizational goals. It includes the desire and ability to understand and respond effectively to other people from diverse backgrounds with diverse views.

Analytical Thinking - is the ability to comprehend a situation by breaking it down into its components and identifying key or underlying complex issues. It implies the ability to systematically organize and compare the various aspects of a problem or situation, and determine cause-and-effect relationships ("if…then…") to resolve problems in a sound, decisive manner. Checks to ensure the validity or accuracy of all information.

POSITION TITLE	Specialist, FOIPP & Information Management	POSITION #:	573847
DIVISION	Corporate Services	LOCATION:	Victoria
PROGRAM:	Records Management	CLASSIFICATION	Grid 27
SUPERVISOR'S TITLE:	Director, Records & Information Management	POSITION #:	573798
SUPERVISOR'S CLASSIFICATION:	Band B	LOCATION:	Victoria

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation. The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

Job Overview

Reporting to the Director, Records & Information Management, the Specialist, FOIPP & Information Management supports the Commission in meeting its legal obligations under the Freedom of Information and Protection of Privacy Act (FOIPPA) and Information Management Act (IMA) through the daily management and administration of Freedom of Information (FOI), proactive release, document discovery, privacy compliance, and information management services.

This position exercises considerable independence, discretion and sound judgement in managing these services on behalf of the Commission. The Specialist supports the Director in achieving strategic goals, corporate objectives and performance targets, and adhering to rigid timelines (legislative and otherwise). In an environment of increasing legislative changes and challenges involving electronic information management, this position works to develop solutions and foster best practices. Diplomatic and service-focussed, this position provides expert leadership, strategic advice, mentoring, guidance, training, and support services to Commission employees in helping them understand and meet their accountabilities under FOIPPA and the IMA. This positions supervises at least one unionized position.

Accountabilities

1. Freedom of Information (FOI), Proactive Release and Litigation

- Manages the Commission's FOIPPA Program;
- Manages all processes associated with the Office of the Information and Privacy Commissioner (OIPC) reviews of complaints, mediation and inquiries, plus litigation document discovery searches and investigations by the Ombudsperson;
- Provides strategic advice and direction to the Commission's Executive, Leadership Group and internal clients on the legislated obligations of FOIPPA as it relates to information access requests (FOI requests) and proactive information releases;
- Manages the internal FOI review, approval, sign-off and release process;
- Implements and manages internal performance standards for FOI administration aligned with legislated requirements and Commission policy and procedures, to ensure FOIPP Program delivery objectives and legal requirements are being appropriately met;
- Develops, implements and manages an internal FOI audit system to measure and evaluate corporate compliance with statutory obligations and Commission objectives, policies and procedures.
- Reviews all requested records for harms prior to release (under FOI or through proactive disclosure), and provides expert advice and direction on the application of FOIPPA to ensure compliance and mitigate risks associated with sensitive issues;

- Leads the development of new internal tracking and reporting systems to effectively manage requests, identify risks or issues, and support Executive reporting and briefings, and corporate statistical requirements;
- Acts in the capacity of the Director, Records and Information Management as and when required for FOIPPA related matters.
- Provides leadership in terms of FOIPPA initiatives, including policy and procedure development, staff training (informal and formal), and other information dissemination initiatives;
- Leads or represents the Commission on inter-governmental committees, working groups and initiatives and represents the RIM business unit on Commission committees, as required.
- Supervises staff by assigning and reviewing work, developing and evaluating performance plans (EPDP's), evaluating work performance, approving leave, responding to grievances, and taking disciplinary action as required; and
- Manages and coordinates the litigation document discovery process for legal matters, as required

2. Privacy

- Leads the establishment of an internal privacy program;
- Develops privacy assessment frameworks for the translation of government's privacy requirements into viable policy, procedural or program changes;
- Manages the completion of Privacy Impact Assessments (PIAs) on new and/or updated corporate programs, legislation, initiatives and systems, as applicable;
- Provides advice on operational privacy matters and mitigation strategies;

3. Information Management (IM)

- Supports the Director in planning and implementing priority activities associated with Commission's long-term IM strategy and legislated accountabilities under the IMA;
- Identifies opportunities to reduce costs, streamline processes, support business needs, and improve stakeholder satisfaction;
- Monitors and assesses internal practices to ensure corporate information is managed in accordance with FOIPPA and other relevant legislation and policies addressing the management of information and records;
- Assists program areas with specific records projects and objectives;
- Provides advice, guidance and day-to-day support to staff on records and information management policies, procedures and standards;
- Develops communications, procedures, methodologies, reports, training materials, presentations and tools for use in projects and initiatives; and
- Delivers training and education to Commission employees.

Organization Chart

Commissioner, Chief Executive Officer
Executive Vice President, Chief Financial Officer
Executive Director, Finance & Administration
Director, Records & Information Management
Specialist, FOIPP & Information Management

Education:

Degree in Library and Information Studies, Information management, Archival Studies, Business or Public Administration, Education, or an equivalent combination of training and work experience; and a minimum of 3 consecutive years of experience administering requests for information under the Freedom of Information and Protection of Privacy Act.

Related Experience:

- Proven experience in the interpretation and application of FOIPPA for access to information (FOI) request processing.
- Experience managing a portfolio of clients in customer service environment with the ability to use tact, diplomacy and sensitivity in handling confidential information, communicating with the public, and working with internal staff on complicated and/or sensitive issues.
- Experience providing advice on policy, procedures and guidelines to staff at all levels.
- Experience establishing, managing or maintaining a records program within a government setting.
- Experience using government records management systems (e.g. TRIM).
- Experience in leading projects and project management.
- Experience in facilitating related training.
- Experience researching/searching, analyzing, and compiling detailed information or reports.
- Experience in managing a diverse and fluctuating workload

Competencies

Service Orientation - Takes personal responsibility for addressing client questions and concerns
Detail Oriented - Sets and attains high standards for quality and accuracy in work
Initiative - Takes the initiative to identify new challenges or opportunities
Process Improvement - Proactively identifies process improvements and takes the appropriate steps to implement them
Problem Solving - Uses critical thinking skills to solve problems and achieve effective solutions
Communication - Ability to clearly convey and receive messages
Teamwork - Working cooperatively and productively with others to achieve results
Focus on Priorities - Is able to identify priority activities and remains focussed on the highest priorities

BRITISH COLUMBIA ENERGY REGULATOR

BC ENERGY REGULATOR
POSITION DESCRIPTION

POSITION TITLE:	Specialist, Digital Information Management	POSITION #:	573861
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Grid 27
Program Area:	Records & Information Services	LOCATION:	Victoria/Fort St John
SUPERVISOR'S TITLE:	Director, Records & Information Management	POSITION #:	573798
SUPERVISOR'S CLASSIFICATION:	Band B	LOCATION:	Victoria

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship, and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation Commission (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

JOB OVERVIEW

The Records & Information Services branch supports the BCER in meeting its mandate and legal obligations in the areas of records management, access, and privacy in accordance with the *Information Management Act* (IMA), *Professional Governance Act (PGA)*, *Freedom of Information and Protection of Privacy Act (FOIPPA)*, and other applicable legislation.

The Specialist, Digital Information Management (Specialist) guides the short and longer-term development, implementation, and maintenance of the corporate records management initiatives with a focus on Microsoft Office 365 (M365) and its technologies. As leader of the Digital Information Management Program, the Specialist provides policy and technical advice to ensure records management policy is upheld; ensures legal and regulatory requirements are adequately met in the M365 environment; oversees the design of departmental SharePoint sites to ensure appropriate management and retention of corporate information; and offers change management support; develops and maintains positive working relationships throughout the BCER; and champions and promotes a strong records management culture and the benefit of mature information management practices.

As a subject matter expert, the Specialist exercises a high degree of independence, discretion, and sound judgement while influencing necessary improvements and changes to digital information governance for the BCER.

ACCOUNTABILITIES

- Develops and implements policy and procedures for records management statutory compliance across the organization particularly within cloud-based solutions, including M365 and its applications.
- Serves in multiple project leadership and management roles to support digital information management program initiatives and adoption of M365 applications.
- Works directly with stakeholders to identify records management business requirements and ensures their translation into information systems and M365 SharePoint design.
- Manages contractors and monitors deliverables to ensure service quality, and delivery on budget within established timelines.
- Leads the design and delivery of corporate-wide training programs on records management compliance and best practices.
- Develops and identifies objectives, targets, and performance measures for records management compliance.
- Provides advice and direction to BCER management and staff regarding information management issues and concerns and participates in planning processes for their resolution.
- Develops and/or facilitates the amendment and approval process of the BCER's Information Schedule (Operational Records Classification System [ORCS]).
- Conducts records management assessments as part of the BCER's Privacy Impact Assessment (PIA) process.
- Supervises and supports records management staff as applicable, by assigning projects and tasks, setting priorities or goals, mentoring and training, approving leave, etc.
- Acts in the role of branch Director, reports to Executive and Leadership, and represents the BCER in external committees and working groups, as required.

ORGANIZATION CHART

Commissioner, Chief Executive Officer
Executive Vice President, People, Reconciliation & Transformation
Vice President, Digital Transformation & Public Trust
Executive Director, Information Systems & Technology
Director, Records & Information Management
Specialist, Digital Information Management (Topic Position)

EDUCATION AND EXPERIENCE REQUIREMENTS

Education:

- Bachelor's degree in Library & Information Studies, Information Management, Archival Studies, Business, Public Administration and 3 years related experience; or,
- An equivalent combination of education, training and experience.

Experience:

- Direct experience with Microsoft Office 365 and SharePoint/Purview as a digital records repository.
- Direct experience with Electronic Document and Records Management Systems (EDRMS).
- Advanced knowledge of BC provincial government records management policy, procedures, and legislation.
- Experience leading complex, large-scale and time-sensitive projects and managing a portfolio of clients.
- Knowledge of change management processes and project management methodologies.
- Experience establishing collaborative relationships with senior management and leading organizational change.
- Proven experience in developing Information Schedules (ORCS) and data retention plans for information system overviews.
- Experience in facilitating training and providing corporate direction on policies, procedures, and legislated requirements.
- Experience and ability to use tact, diplomacy, and sensitivity in handling confidential information and issues.
- Experience in managing a diverse and fluctuating workload.

KEY COMPETENCIES

Service Orientation – Takes personal responsibility for addressing client questions and concerns.

Teamwork & Cooperation – Is able to work cooperatively within diverse teams, work groups and across the Regulator to achieve operational goals and results.
Problem Solving – Uses critical thinking skills to solve problems and achieve effective solutions.
Communicates Strategy & Rationale – Is able to effectively communicate vision and rationale behind decisions and policies.

POSITION TITLE:	Records & Information Management Analyst	POSITION #: 573247	
DIVISION:	Corporate Services	CLASSIFICATION: Grid 15	
Program Area:	Records & Information Management	LOCATION: Victoria	
SUPERVISOR'S TITLE:	Specialist, EDRMS & Info Management Solutions	POSITION #: 573861	
SUPERVISOR'S CLASSIFICATION:	Grid 24	LOCATION: Victoria	

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

JOB OVERVIEW

The BC Government's information management landscape is undergoing modernization and significantly transforming the way that public bodies must manage their recorded information, with heightened focus on compliance, digitization/electronic records management, and alignment with Government's commitment to openness and transparency. The Records and Information Management (RIM) unit provides leadership, direction and support to the Commission in meeting new legal requirements for electronic information management under the new *Information Management Act (IMA)*, and information access and privacy protection obligations in accordance with *The Freedom of Information and Protection of Privacy Act (FOIPPA)*.

The Records and Information Management (RIM) Analyst is a key member of the Commission's Records and Information Management (RIM) business unit. Under the direction of the RIM Director, this position is responsible for a broad range of records and information management (RIM) functions focused on achieving legislative compliance, promoting best practices, mitigating risks, improving operational efficiency, and developing customized solutions to RIM challenges to effect positive change and support the availability, integrity, accuracy and effective management of client information assets.

ACCOUNTABILITIES

- Provides advice to a diverse corporate client base on the interpretation, application and impact of BC's new Information Management Act (IMA), and government's supporting policies, standards and procedures.
- Takes a leading role within the Commission to promote awareness and understanding of the changing landscape of recorded information management under the IMA (electronic/digital information management and change management focus).
- Leads clients towards finding appropriate solutions to challenges related to managing electronic data/information by developing, implementing and/or guiding the implementation of electronic file plans and document naming conventions for shared network folders and documents, and for application within data systems.

- Contributes to the ongoing testing and improvement of corporate information systems (e.g. IRIS, Kermit) and provides feedback to database developer(s) with respect to data issues, upload/download activities, etc. to support positive user experiences and functional efficiency.
- Applies expert knowledge of digital records management applications and technology, and industry-approved standards for digitization of Commission original physical records.
- Analyzes and reviews oil and gas industry data types (such as LAS, XML and PAS files) and other digital data for quality/integrity/standards/issues prior to external publishing to e-Library and/or applicable FTP sites in support of the Business Transformation Strategy (BTS) and other proactive release requirements.
- Provides project management leadership and/or support to client information management projects, ensuring Commission information assets are managed effectively in accordance with their value and as required by current legislation, policy, standards and procedures.
- Identifies information, communication and training needs to develop resources, educational materials and communication tools, including web content for intranet and extranet sites.
- Develops and delivers and/or assists in the delivery of records and information management training.
- Contributes to the development of disaster preparedness and recovery plans.
- Researches policy developments and best practices on the management of digital information, and recommends enhancements to current policies and procedures as corporate business functions, legislation or government-wide policies and procedures are introduced or amended.
- Researches oil and gas industry (e.g. well, field and pool, etc.) legislation, regulations, policy and procedures as they apply to external stakeholder inquiries and requests.
- Provides input to the development of new corporate records and information management policy.
- Provides expert advice and guidance to internal clients on a daily basis about the classification, creation, retention, retrieval and disposition of records and data in accordance with ARCS and ORCS.
- As a first point of contact for information requests from industry/external stakeholders, provides expert support for service desk requests involving complex and high volume data searches and/or troubleshooting and time-sensitive issues.
- Interprets and effectively responds to issues, queries and requests for information from internal and external client stakeholder groups through a range of communication channels, ensuring corporate service standards for timeliness, prioritization, accuracy, and quality of response are achieved.
- Using expert knowledge of Commission operational records, RIM best practices and confidentiality principles applied to corporate records and business data, reviews requested information prior to release to prevent risks associated with unauthorized disclosure.
- Conducts audits and reviews to assess compliance on records and information management practices and processes, and develops recommendations for improving efficiency and reducing risk.
- Applies business and records management knowledge to contribute to the development and review of the Commission's Operational Records Classification System (ORCS).
- Approves disposition (including destruction or preservation) of non-transitory scheduled client recorded information as the Commission's alternate Corporate Records Officer.
- Monitors, tracks and reports on expenditures, progress, and timelines related to RIM contracts and projects and storage, imaging, and disposal services, as required.
- Establishes and maintains multiple, complex registries of active and semi-active corporate record holdings stored onsite, or in various government-contracted location and Commission offices/facilities.

ORGANIZATION CHART

Commissioner, Chief Executive Officer
Executive Vice President, Chief Financial Officer
Executive Director, Finance and Administration
Director, Records & Information Management
Specialist, EDRMS & Info Management Solutions
Records & Information Management Analyst (Topic Position)

EDUCATION AND EXPERIENCE REQUIREMENTS

Education:
High school diploma supplemented with post-secondary courses in records management, archival studies, business or public administration plus three years of related experience.; OR technical diploma in records management, archival studies or closely related discipline and two years of related experience; OR degree in library or archival studies, business, public administration, management and one year of related experience.

Experience:
- Progressive experience in data, document and information management (e.g. classification, scheduling, transfers and retrievals, disposition, digitization/imaging technology, governing legislation, technical standards, etc.).
- Experience in providing on-going advice and guidance to staff of all levels on records management policies, procedures, standards and best practices.
- Ability to liaise effectively with internal and external stakeholders, such as internal business groups and members of the oil and gas industry.
- Experience in managing administrative and operational records in various formats according to ARCS and ORCS and/or approved records schedules.
- Experience with managing projects, including providing technical direction to staff.
- Demonstrated experience and ability to organize, manage and complete a number of concurrent projects.
- Strong ability to demonstrate tact, discretion, and sensitivity when dealing with clients, stakeholders, sensitive situations and confidential material.
- Ability to maintain strict confidentiality.
- Ability to ensure a high standard of accuracy in all levels of work.
- Ability to work independently or in a team environment, under significant pressure and meet deadlines.

Knowledge:
- BC Information Management Act (IMA) and associated policies and procedures
- BC Government Records and Information Management Manual
- BC Government Administrative Records Classification System (ARCS) and BC Oil and Gas Commission's Operational Records Classification System (ORCS)
- Commission policies, procedures and guidelines relating to records and information management, eSubmission and oil and gas activities.
- Oil and Gas Activities Act (OGAA) and other related sector legislation and regulations.

KEY COMPETENCIES

Service Orientation - Takes personal responsibility for addressing client questions and concerns
Detail Oriented - Sets and attains high standards for quality and accuracy in work
Initiative - Takes the initiative to identify new challenges or opportunities
Process Improvement - Proactively identifies process improvements and takes the appropriate steps to implement them
Problem Solving - Uses critical thinking skills to solve problems and achieve effective solutions
Communication - Ability to clearly convey and receive messages
Adaptability - Willingness and ability to effectively work in and adapt to change
Teamwork - Working cooperatively and productively with others to achieve results
Focus on Priorities - Is able to identify priority activities and remains focused on the highest priorities

POSITION TITLE:	Well File Technician	POSITION #:	573268
DIVISION:	Corporate Services	CLASSIFICATION:	Grid 15
Program Area:	Finance and Administration	LOCATION:	Victoria
SUPERVISOR'S TITLE:	Specialist FOIPP and Information Management	POSITION #:	573847
SUPERVISOR'S CLASSIFICATION:	Grid 27	LOCATION:	Fort St. John

The BC Oil and Gas Commission (Commission) is the provincial single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

JOB OVERVIEW

The principal functions of the Well File Technician are to provide expert administration and management of technical well data including ensuring industry compliance with regulations and guidelines, coordination of the public release of data from confidential status, and the development, implementation and management of all aspects of best practices and procedures relating to well data document management. The position contributes to the management and exploration of the Province's petroleum and natural gas operations by responding to industry queries regarding well data. The position also oversees the categorization, recording and tracking of all incoming technical well data using a complex document management system, and manages staff to carry this out.

ACCOUNTABILITIES

- Responsible for compliance to ensure that required data is submitted in the formats and timeframes stipulated by regulation and OGC guidelines, and contributes to the development of those guidelines;
- Interprets regulations and develops guidelines for compliance of well data submissions;
- Develops, implements and maintains procedures and processes in accordance with generally accepted Document Management best practices, applying document management expertise relating to all aspects well data document management including but not limited to document processing, submission requirements, compliance and enforcement, scanning and imaging, etc.;
- Responsible for the implementation of the scanning and imaging of well data and logs and the overseeing of the scanning well data and logs into appropriate electronic applications;
- Coordinates the timely review, recording, approval and communication for all core and sample removal applications. Carries out the designated OGAA approval where applicable;
- Oversees the categorization, recording and tracking of all incoming technical well data, including the transfer of digital data into appropriate locations;
- Responds to enquiries from Canadian Association of Petroleum Producers (CAPP), Canadian Association of Petroleum Information Specialists (CAPIS) and other petroleum data vendors regarding information pertinent to the oil & gas exploration activities in British Columbia;

- Researches, plans, develops, and implements consistent Records Management Functions across worksites;
- Develops the procedures / processes to bring the OGC up to current recognized best practices in order to ensure the completeness of the well files and that the information captured is reliable and accessible over time and location.

ORGANIZATION CHART

Commissioner, Chief Executive Officer
Executive Vice President, Chief Financial Officer
Executive Director, Finance and Administration
Director, Records and Information Management
Specialist, FOIPP and Information Management
Well File Technician (Topic Position)

EDUCATION AND EXPERIENCE REQUIREMENTS

Education:

- High school diploma supplemented with post secondary courses in records management, archival studies, business or public administration plus 3 years of related experience.; OR
- Technical diploma in records management, archival studies or closely related discipline and 2 years of related experience; OR
- Bachelor's degree in library or archival studies, business, public administration, management and 1 year of related experience;
- There will be different combinations of relevant experience, education and/or training that would result in an applicant meeting the above standards.

Experience:

- Progressive experience in document management, records management and scanning and imaging;
- Must have established, guided and provided on-going advice regarding the records and document management and the scheduling of records which ensures systematic organization, retrieval, storage, destruction or permanent destruction;
- Management of administrative and operations records including paper files, microfilm, diskettes, magnetic tape, electronic data processing records, and video or audiotapes; and
- Supervising staff.

KEY COMPETENCIES

Service Orientation - displaying a desire to identify and serve customers/clients, who may include the public, colleagues, partners (e.g. educational institutes, non-government organizations, etc.), co-workers, peers, branches, ministries/agencies and other government organizations and focusing one's efforts on discovering and meeting the needs of such customers/clients.

Results Orientation - showing concern for surpassing a standard of excellence, be it one's own past performance (striving for improvement); an objective measure (achievement orientation); challenging goals one has set; or even improving or surpassing what has already been done (continuous improvement).

Teamwork and Cooperation - demonstrates the ability to work co-operatively within diverse teams, work groups and across the organization to achieve group and organizational goals.

Concern for Order - reflects an underlying drive to reduce uncertainty in the surrounding environment. It is expressed as monitoring and checking work or information, insisting on clarity of roles and functions, etc.

_____ _____

DATE **EXCLUDED MANAGER SIGNATURE**

BRITISH COLUMBIA ENERGY REGULATOR

BC ENERGY REGULATOR
POSITION DESCRIPTION

POSITION TITLE:	Records Coordinator	POSITION #:	573906/573907
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Grid 12
PROGRAM AREA:	Records & Information Services	LOCATION:	Fort St. John
SUPERVISOR'S TITLE:	Specialist, FOIPP & Information Management	POSITION #:	573847
SUPERVISOR'S CLASSIFICATION:	Grid 27	LOCATION:	Fort St. John

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation BCER's (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

JOB OVERVIEW

The Records Coordinator (Coordinator) provides hands-on support in the Records & Information Services Branch. Under the direction of the Specialist, FOIPP, this role is responsible for coordinating and maintaining the storage, access, use, and disclosure of BCER records, both electronic and paper. The Coordinator responds to requests for records and information received from internal and external stakeholders, by locating and digitizing (scanning) a high volume of paper files and documents in a timely manner. This role provides exceptional customer service in a busy environment while dealing with a variety of confidential and sensitive materials. This position also provides back-up coverage for the Receptionist in the Fort St. John office when required.

ACCOUNTABILITIES

- Maintains the efficient operation of the Fort St. John Records Centre on a day-to-day basis by ensuring BCER files and documents are appropriately maintained in accordance with established best practices. This includes:
  - Filing, classifying, organizing, putting into inventory, and culling records in accordance with ARCS and ORCS retention schedules, and government standards.
  - Responding to a high volume of time sensitive requests and correspondence as the first point of contact.
  - Interpreting client requests for copies of BCER records and responding with speed and accuracy, in accordance with applicable policies, procedures, and legislation.
  - Understanding of requests and data retrieval actions required as related to Freedom of Information and legalities of request.

- Applying a sound understanding of BCER records, recordkeeping systems, and information systems to ensure accurate and complete responses.
- Reviewing requested information prior to release and making appropriate decisions on withholding personal and/or confidential information from disclosure in accordance with the Freedom of Information and Protection of Privacy Act (FOIPPA) exceptions to disclosure.
- Providing on site coordination and support for records access and digitization activities to external clients and/or contractors as required.

- Works with scanners/imaging equipment to convert high volumes of paper records into digital copies in accordance with established standards.
- Applies technical skills and a knowledge of BCER systems (IRIS, Kermit, AMS, FTP sites, Service Desk, etc.) to efficiently search/locate, copy, download, consolidate, and release electronic records in response to requests.
- Provides back-up coverage for the Fort St. John office Receptionist position as and when needed; coverage may include receiving, screening and appropriately directing incoming calls, greeting walk-in clients and visitors, coordinating mail/courier services, and assisting with boardroom bookings.
- Establishes, maintains, and promotes positive relationships with BCER staff, clients, and external stakeholders.
- Performs other related duties required or assigned.

ORGANIZATION CHART

Commissioner, Chief Executive Officer
Executive Vice President, People, Reconciliation & Transformation
Vice President, Digital Transformation & Public Trust
Executive Director, Information Systems & Technology
Director, Records & Information Management
Specialist, FOIPP & Information Management
Records Coordinator *(Topic Position)*

EDUCATION AND EXPERIENCE REQUIREMENTS

Education:

- Completion of Grade 12 or equivalent, supplemented with courses in records management; archival studies, business, or library sciences plus two or more years of related experience; *OR*
- Technical diploma in records management, archival studies or closely related discipline and two years of related experience; *OR*
- A combination of three years of administrative support experience, education and/or training.

Experience:

- Demonstrated experience working with a recordkeeping or filing system for paper and/or electronic records where best practices were applied. Preference to candidates with knowledge of records management best practices as it applies to BC public bodies and ARCS/ORCS.
- Demonstrated ability to interpret policies and follow standard procedures.
- Experience with Microsoft Office products and using a range of information systems.
- Experience in managing and prioritizing multiple work tasks in a high-pressure setting, while exercising a high degree of accuracy and professionalism.
- Experience working in a customer service-focussed environment and providing excellent service levels.
- Demonstrated ability to act in a professional and respectful manner and contribute to a positive work environment.

Given the nature of this position, it is required to work in the Hub Office. Must be able to lift up to 30 lbs

KEY COMPETENCIES

Communication - Ability to clearly convey and receive messages
Teamwork - Working cooperatively and productively with others to achieve results
Service Orientation - Takes personal responsibility for addressing client questions and concerns
Detail Oriented - Sets and attains high standards for quality and accuracy in work

Information Management Foundations

BRITISH COLUMBIA ENERGY REGULATOR

Welcome to the Information Management Foundations eLearning course. This course will familiarize you with the basics of information management, including an understanding of:

- What government information is;
- Your FOIPPA responsibilities; and
- Privacy awareness

St. Mark's Summit, West Vancouver

Adventures in...

Records Management

The BC Energy Regulator (BCER) is the steward of a significant amount of government information, and we all have an important role in creating a culture of efficient and effective information management. This section provides guidance about information management obligations and best practices that are essential to the work of all BCER employees.

Upon completion of this topic, learners will be able to:

- Understand what government information is, and the value of records and data
- Describe the benefits of good record keeping practices
- Know their responsibilities to maintain evidence of business activities, transactions and decisions
- Recognize which records are transitory and the information schedules available for managing records
- Apply best practices around the management of records, including email

Show less

START MODULE

Privacy

What are our responsibilities as public servants when it comes to the personal information that we hold? This section provides principles and guidance that will help us treat personal information responsibly and lawfully.

Upon completion of this topic, learners will be able to:

- Understand what personal information is
- Apply privacy principles to the work of the BCER
- Know how to identify and respond to an information incident

- Find privacy resources such as the Privacy Impact Assessment template and Guideline

Show less

START MODULE

Access to Information

The Freedom of Information and Protection of Privacy Act (FOIPPA) provides individuals a right to access their own personal information held by public bodies, as well as general information about BCER operations, programs and services – with limited exceptions. This section describes the formal "FOI" process, as well as the proactive disclosure of government information outside of the FOI process.

Upon completion of this topic, learners will be able to:

- Recognize the obligations placed on public servants when responding to FOI requests
- Understand the roles and responsibilities of everyone involved in a FOI request
- Know how to perform an adequate search for records
- Differentiate between a FOI request and proactive disclosure

Show less

START MODULE

Contact Records and Information Services

This learning program is adapted from BC Governments IM117 course.

Records Management

What is government information?

Let’s start with defining our terms: what do we mean by ‘government information’?

Government information is recorded information in any format that is created or received by a government body (BCER) in connection with government business, including data and records. In this learning program, the term ‘government information’ applies to information we hold in the BCER. It is the official and legal term for the information the BCER uses, creates and receives in the course of our day.

Records – What is Government Information?

Identify which of the following may contain government information.
Select all that apply:

- [ ] Case management system entries
- [ ] Voicemail messages
- [ ] MS Teams chats
- [ ] Instant messages
- [ ] Handwritten notes
- [ ] Reports
- [ ] Email messages
- [ ] Maps
- [ ] Policies
- [ ] Statistical data

SUBMIT

DOWNLOAD WHAT IS GOVERNMENT INFORMATION ACTIVITY DESCRIPTION

All employees are required to manage BCER information according to information schedules, relevant policies, and legislation. There are many recordkeeping practices that can be applied every day. In this section, we’ll cover the basics, and good practices you need to know.

See here for a glossary of records management definitions.

Why do we create records?

The information we create and receive is fundamental to good government and accountable public administration. Adequate records and reliable practices support efficiency and the delivery of quality services. Records and data are enterprise assets that must be managed according to their value.

They can have different values:

- Administrative
- Operational
- Evidential
- Legal
- Informational
- Financial and audit
- Historical

We rely on records every day to support the work we do. They may document key decisions and they require our care and attention.

Please keep in mind that when you're at work, you might also create or receive information that is not related to your work. Keep this information to a minimum and separate from BCER information.

> Exercise: Take a minute to consider the records you interact with during your everyday work. Who relies on the information in those records? Do you understand their impact on individuals and society? And where are they kept?

What is our framework for managing records?

To understand the framework for managing records, we need to be aware of current and updated legislation and policy, as well as standards, guides, and resources. Let's introduce some of the key parts of our framework.

The Information Management Act (IMA) is government's primary information management law, and applies to the BC Energy Regulator.

What does the IMA do? The IMA is the Province's legislative framework for digital information practices. It modernizes and streamlines government information management by:

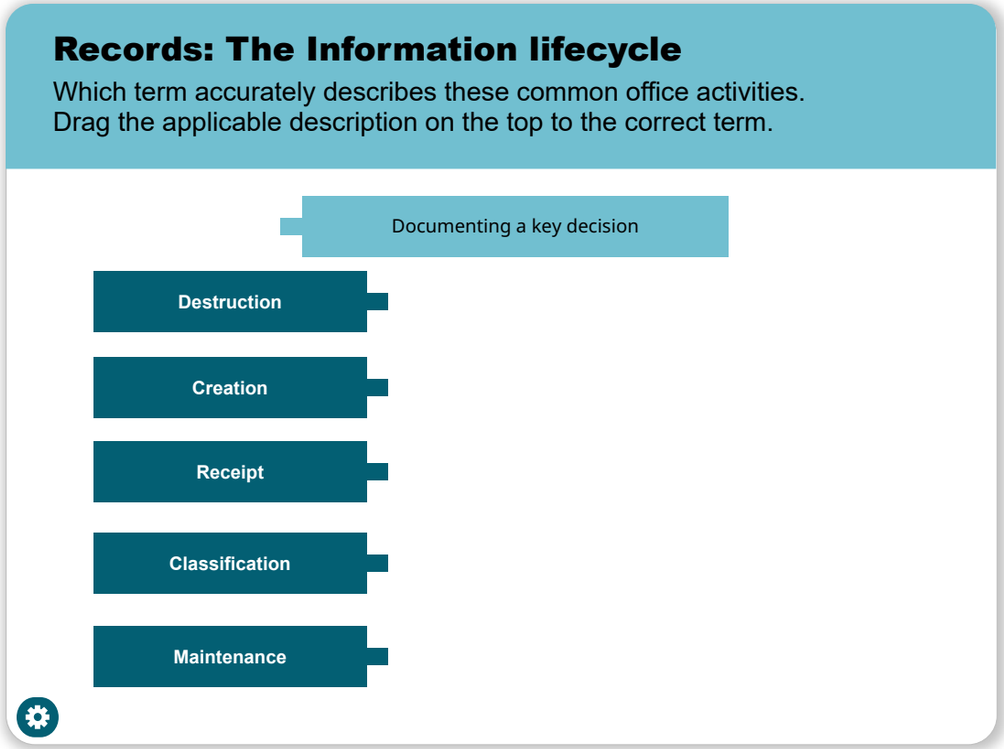
- Transitioning government to the digital storage and management of information
- Establishing digital archives and requiring the archiving of information in digital form (subject to reasonable exceptions)
- Establishing a Chief Records Officer to approve information schedules, manage the digital archives and to promote effective information management across government
- Establishing an obligation to ensure that an appropriate system is in place to create adequate records of government decisions, and to manage and secure all government information from creation to disposal or archiving

In short, the IMA supports productivity, cost reduction, timelier services for the people of British Columbia, and improved access to information.

The BCER's Information Management Policy helps staff understand their information management (IM) obligations as they relate to IMA requirements. Policy requirements are established for the full lifecycle of information. We recommend staff read this policy.

The information lifecycle

The information life cycle is the life span of a record from its creation or receipt to its final disposition. A record's lifecycle includes three main phases: active, semi-active, and final disposition. During this life cycle a record may be created, received, classified, scheduled, maintained, used, stored, destroyed and/or transferred for permanent retention in the government archives.



DOWNLOAD THE INFORMATION LIFECYCLE ACTIVITY DESCRIPTION

Documenting decisions

You must take reasonable steps to ensure that adequate records of decisions are created and maintained.

It’s important that the Regulator manages information so it’s reliable and available to those who need it, and to ensure that it’s kept for the required length of time.

The IMA establishes an obligation to ensure that an appropriate system is in place to create adequate records of government decisions. Under the IMA, the Chief Records Officer has issued a directive and guidelines to assist government bodies in meeting their obligations related to documenting their decisions.

In general, a record of decision is adequate if someone who's not familiar with the decision could be reasonably informed about the decision.

Carefully consider what is required to adequately document a decision. In some cases, an adequate record of a decision may be a brief note in a case management system or a case file; in other cases, it may be made up of numerous extensive studies.

Ensure you're storing records of decisions and the records you create in the most appropriate place in your office's recordkeeping system. Office recordkeeping systems do not include locations that are only available to you, such as your email account or desktop.

The BCER does not have to create and keep records of every decision made by every employee. BCER staff need to identify which decisions are to be documented by applying your judgement in the context of our specific mandates and with consideration to the purpose and intent of the IMA, the directive and the guidelines, and other obligations that may exist in law and policy respecting documenting decisions.

Why document decisions?

- Supports openness and transparency
- Facilitates effective decision making
- Preserves corporate memory
- Supports employees in doing their jobs effectively and providing high quality services to the public
- Supports accurate reporting of decisions to stakeholders, including other government bodies and the public
- Contributes to the Province's historical record for future generations

Records: Documenting decisions

Which of the following statements are true for government bodies?
Select all that apply.

- ◯ Must use appropriate systems for maintaining adequate records of decisions
- ◯ Should ensure that key decisions are securely maintained on personal drives
- ◯ Does not have to create and keep records of every decision made by every employee
- ◯ Needs to identify which decisions are to be recorded by considering context, the purpose and intent of the IMA, CRO directives and guidelines.

DOWNLOAD DOCUMENTING GOVERNMENT DECISIONS ACTIVITY DESCRIPTION

See here to learn more about the Documenting Government Decisions CRO Directive and Guidelines.

See here for Regulator Documenting Decisions guidance.

Shared responsibility

BCER staff are responsible for documenting their work by ensuring records they create or receive are adequate, and are filed in their office recordkeeping system, including email.

Program areas are responsible for maintaining a shared office recordkeeping system that’s organized and administered in accordance with information management legislation and policy.

Your office recordkeeping system does not include locations that are only available to you, such as your email account, computer hard drive, OneDrive or desktop.

And remember, the directive and guidelines for Documenting Decisions specifically define the requirements for creating and maintaining government information that is an adequate record of a government body’s decisions.

Common types of recordkeeping systems include:

A Shared Drive structure with ARCS and ORCS applied; line of business applications, organized and governed SharePoint sites, and physical filing systems (e.g. paper in the FSJ Records Centre).

Scenario – cleaning up email before going on vacation

Drew is going on vacation for three weeks and has been working on several time-sensitive projects and keeping their work in personal drives and email. Feeling overwhelmed, Drew reaches out to Maria, who has excellent records management habits.

What advice would Drew get from Maria?
Select the best option.

- ○ **Option A)** To leave the records as they are or send anything important to Maria as an email attachment just in case.
- ○ **Option B)** To review their project email and files, to delete duplicate information and to identify final email and email chains that contain the complete record and to save them in the team's shared project file, including any substantive notes and drafts or final documents.

SUBMIT

DOWNLOAD CLEANING UP YOUR EMAIL BEFORE GOING ON VACATION ACTIVITY DESCRIPTION

Information schedules

Information schedules are our primary tools to manage government information effectively over time. They:

- Describe and classify government information
- Set out the final disposition of a record (that is, whether it will ultimately be transferred, archived or destroyed)

- Are approved under the IMA
- Increase efficiency
- Uphold the trust that comes with the obligation to protect government information

Understanding schedules is critical to help your organization meet its obligations under the IMA. In the BCER, we use ARCS, ORCS (the Oil and Gas Regulation Operational Records Classification System), and Special Schedules, such as the Transitory and Executive Records Schedules.

Click on the three main types of schedules below to see why each is important to your work.

ARCS

ORCS

Special Schedules

DOWNLOAD THREE MAIN TYPES OF INFORMATION SCHEDULES ACTIVITY DESCRIPTION

Transitory information

Transitory information is information of temporary usefulness that's needed only for a limited time to complete a routine action or prepare a final record. It can exist in any format or medium (paper or digital) and can be created and shared using a variety of technologies (e.g., email, social media, Teams, SharePoint).

By promptly removing transitory information (also known as transitory records), employees are better able to identify and file key records into their recordkeeping system, where they can be easily found. As well, the BCER avoids unnecessary costs for storing and processing transitory records. Transitory records are covered by the Special Schedule for Transitory Records (schedule 102901). They do not need to be filed using ARCS or ORCS.

Who can apply the Transitory Records schedule? You! The authority to identify transitory records is delegated to each B.C. public servant. Transitory information can and should be disposed of when it's no longer of value, with one important exception: if the Regulator receives an FOI or litigation search request, all relevant records must be provided, including transitory information that exists at the time of the request. Transitory information that's subject to such requests must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities.

Use this Transitory Records Guidance to determine whether the information is transitory.

A record's content and context determine whether it is transitory, not its format or storage medium. If an email, draft document, or other record is essential to understanding the Regulator's business – e.g. how a particular decision was reached – then the record is not transitory and must be kept.

Which of these statements are true?

Select all that apply.

- [ ] All instant messages are transitory
- [ ] Transitory information can be destroyed when no longer needed, unless it is relevant to a search for legal purposes, or an active FOI request
- [ ] Deleting information makes it transitory
- [ ] Records containing transitory information are subject to FOI

Submit

DOWNLOAD TRANSISTORY INFORMATION ACTIVITY DESCRIPTION

Creating and managing email

All employees are encouraged to follow email management best practices, as set out in the email guidance on the Energy Exchange.This material provides detailed information on using your email account, including sending, searching and managing email, and protecting sensitive information. If you apply these and other best practices, it will make it easier to find the information you need, while also ensuring that information is available to your colleagues when you are not in the office, and in the event of an FOI request or litigation search.

Creating and Managing Email

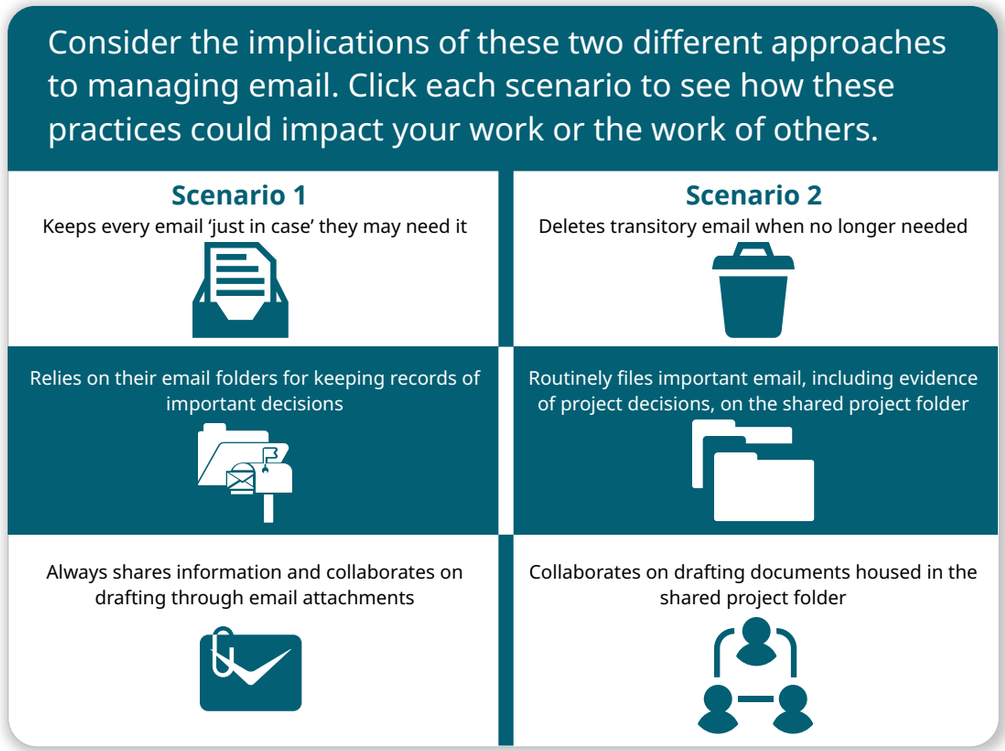
DO	DON'T
Regularly file email that is material to business operations and decisions in the office recordkeeping system	File transitory emails
Use separate email threads for different subjects	Create unnecessary email and email attachments
Use meaningful and concise subject lines	Use your personal email accounts for BCER business
Regularly dispose of transitory email and utilize Outlook tools and features to help (e.g., the "clean up conversation" tool)	Rely solely on email and similar technologies when making important decisions, and if you do use email, ensure that the email adequately documents a decision and make sure to file it
Keep personal use of your BCER email account to a minimum	Triple delete emails

DOWNLOAD CREATING AND MANAGING EMAILS ACTIVITY DESCRIPTION

It's important to remember, when you file email into your recordkeeping system, the original email in Outlook is redundant and should be deleted. Not doing so may cause confusion as to which copy is the official record.

Do I need to keep every email? When can I delete an email?

You need to save all emails that pertain to the business of the Regulator, except for transitory emails. You may delete transitory emails when they're no longer needed. You must not delete any emails that may be responsive to an active FOI request or request for legal discovery. You should save emails that document an important government decision.



DOWNLOAD TWO DIFFERENT APPROACHES TO MANAGING EMAILS ACTIVITY DESCRIPTION

Disposal of BCER information

We've already established that information schedules govern how long records are needed and when they may be appropriately archived, disposed of or transferred to another organization. The BCER Records and Information Services Branch manages the disposal of information through the transfer of records to the government archives, or following our Documented Destruction Process.

How do we Dispose of Information

Disposal of government information must be carried out in a **secure** and **confidential** manner.

The more **sensitive** the information is, the more measures we should take to ensure that it is **securely** and **appropriately destroyed**.

DOWNLOAD HOW TO DISPOSE OF INFORMATION ACTIVITY DESCRIPTION

Resources

BCER's Records and Information Services (RIS) is committed to providing services, resources and learning tools that support you and the BCER. Our Energy Exchange pages contain guidance on everything we covered in this section and more.

RIS is here to help you with the following services:

- Records management advice for all types of records
- Online guides and eLearning
- Information schedule advice
- Shared Drive Organization and Collaborative Digital Workplace (SharePoint) projects
- Accessing physical records

We encourage you to contact RecordsManagement@bc-er.ca for assistance.

CLOSE THIS TAB

Privacy

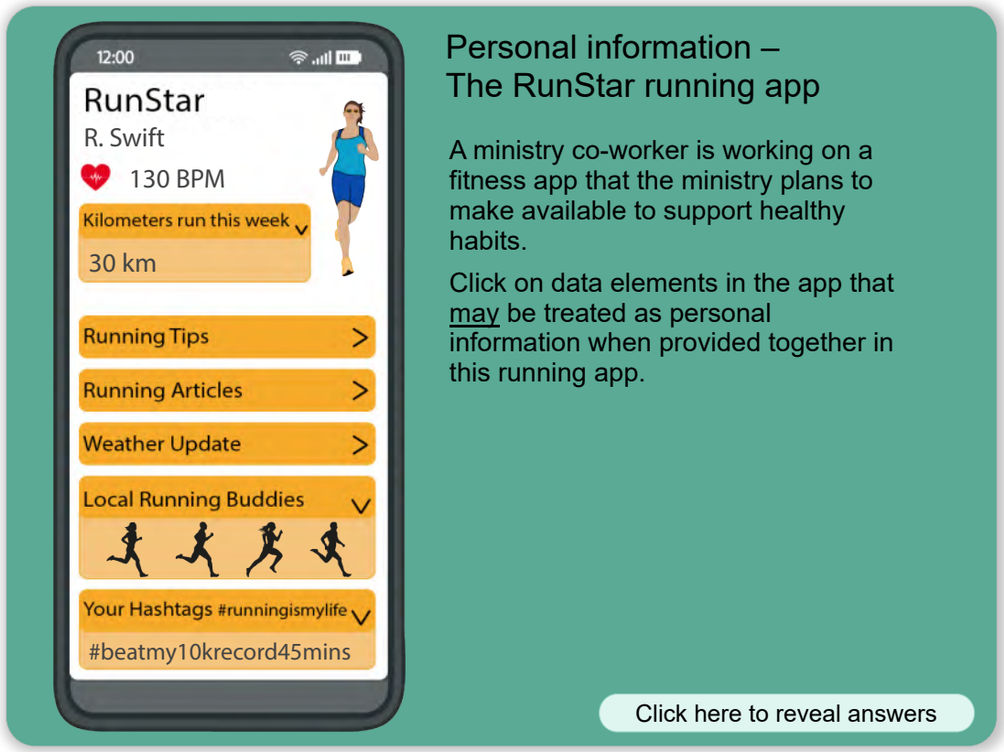
The Freedom of Information and Protection of Privacy Act (FOIPPA) outlines the circumstances in which public bodies, such as BCER, can collect, use and disclose personal information. FOIPPA requires that all public servants protect the personal information that we hold. Privacy is a complex topic. This course supports BCER employees with an understanding of how to handle personal information responsibly and lawfully.

What is personal information?

Personal information is recorded information about an identifiable individual other than their business contact information. Personal information can include things like someone's name, home address and home email. It also includes their educational history, employment history, and even their personal opinions.

Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used or disclosed. Sensitive personal information is not defined in FOIPPA. Some examples of what may be considered sensitive personal information include: DNA, personal health history, information about sexual orientation, gender identity, religious or political beliefs, and race or ethnicity.

All personal information must be treated as confidential information.



DOWNLOAD PERSONAL INFORMATION ACTIVITY DESCRIPTION

Business contact information

Personal information does not include business contact information – information that enables you to contact someone for work purposes – such as a name, work phone number or email address. Yet, some contact information can be considered personal if it's being used for personal reasons.

Click the buttons below to review the Scenarios

Scenario 1

Scenario 2

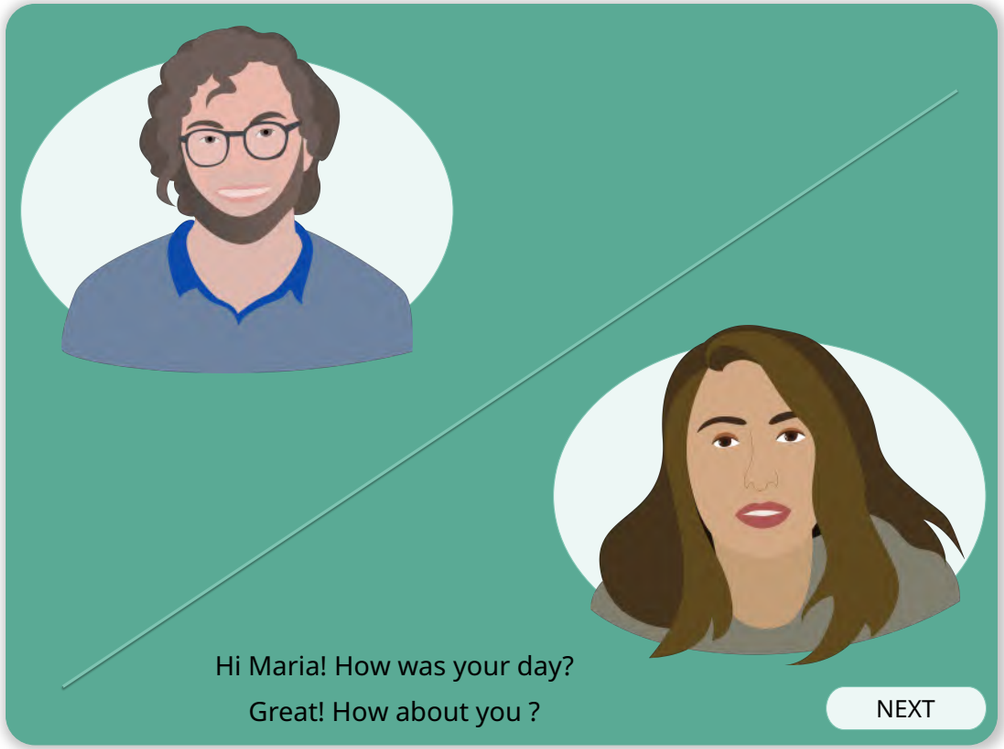
DOWNLOAD BUSINESS CONTACT INFORMATION ACTIVITY DESCRIPTION

The mosaic effect

The mosaic effect occurs when information that appears to be non-identifiable is combined in a way that can reveal the identity of an individual. For example, an email address may not contain an individual's name but when you can see information that email address is associated with (e.g., website user accounts set up by that email), you might be able to identify the email address's owner. If you can combine information about an individual's hobbies and hometown you may not be able to identify anyone if they are an avid foodie from Vancouver but an elite trampolinist from Oliver, B.C. might be more easily identified.

Think about the mosaic effect when seeking to understand privacy implications. While medical records, dates of birth and home addresses are easily recognizable as personal information, individuals can often be identified within data that has been de-identified.

Consider the mosaic effect in this conversation about a hiring competition that Drew is managing.



DOWNLOAD MOSAIC EFFECT IN A CONVERSATION ACTIVITY DESCRIPTION

Freedom of Information and Protection of Privacy Act

As employees of a public body bound by FOIPPA, we are all responsible for ensuring that our work is carried out in accordance with B.C.’s privacy legislation.

You may have access to personal information that your program area has collected for an authorized purpose. B.C. public servants can only access, use or disclose personal information where required and authorized to do so for work; we cannot do so for our own purposes. Accessing information without the

appropriate authority may result in an information incident that would need to be reported.

FOIPPA also requires that public bodies protect personal information. The BCER does this by using reasonable security controls, ensuring that individuals who handle personal information are aware of their responsibilities, and completing privacy impact assessments.

Privacy principles at work

As B.C. public servants, we need to handle personal information appropriately. When you access personal or other confidential information, consider how your plans for the information align with privacy principles.

You can find out more about privacy principles here: Ten Privacy Principles

Privacy principle: Identify purpose

Select the questions that you should ask yourself that are related to the above principle.

- ◯ Why do you need the personal information?
- ◯ Is all of it needed for the task at hand?
- ◯ Did you get this personal information from an appropriate source?
- ◯ What are you doing to protect the information while you access it?
- ◯ Are you using information for a legitimate purpose?
- ◯ Before you share information, how do you know it's okay to share it?

Privacy impact assessments

Privacy impact assessments (PIAs) are tools to evaluate the privacy implications of new and existing enactments, systems, projects, programs or activities. PIAs must be started early in the development process for new initiatives that the BCER introduces and any changes that are to be implemented. Complete PIAs before the program is launched and always before any personal information is collected, used or disclosed.

PIAs promote transparency, accountability, and contribute to continued public confidence in the way the government manages personal information.

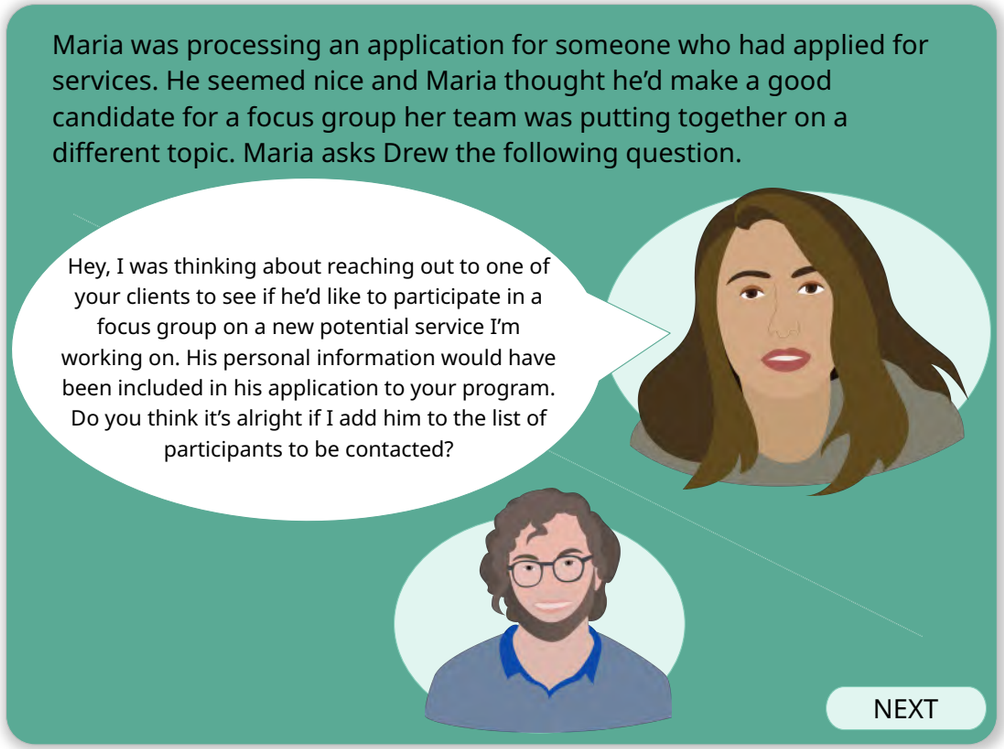
Starting a new project

Maria is helping to design a new program to provide services for residents. How can they ensure privacy is considered appropriately in this new program? Select all that apply and click SUBMIT:

- [ ] Start collecting the personal information that's available. Information that's not necessary can be deleted later
- [ ] Reach out to the Privacy Officer
- [ ] Draft a PIA, even if there are still details to be worked out
- [ ] Email the PrivacyOfficer@bc-er.ca to be granted your FOIPPA authorities

SUBMIT

DOWNLOAD STARTING A NEW PROJECT ACTIVITY DESCRIPTION



DOWNLOAD PROCESSING AN APPLICATION ACTIVITY DESCRIPTION

Information incidents

An information incident is a single or a series of events involving the collection, storage, access, use, disclosure or disposal of government information that threaten privacy or information security and or contravene law or policy. Information incidents can involve confidential or personal information. A privacy breach is a type of information incident.

Reporting information incidents

If you discover or suspect an information incident, report it immediately by calling the BCER Privacy Officer, or email PrivacyOfficer@bc-er.ca.

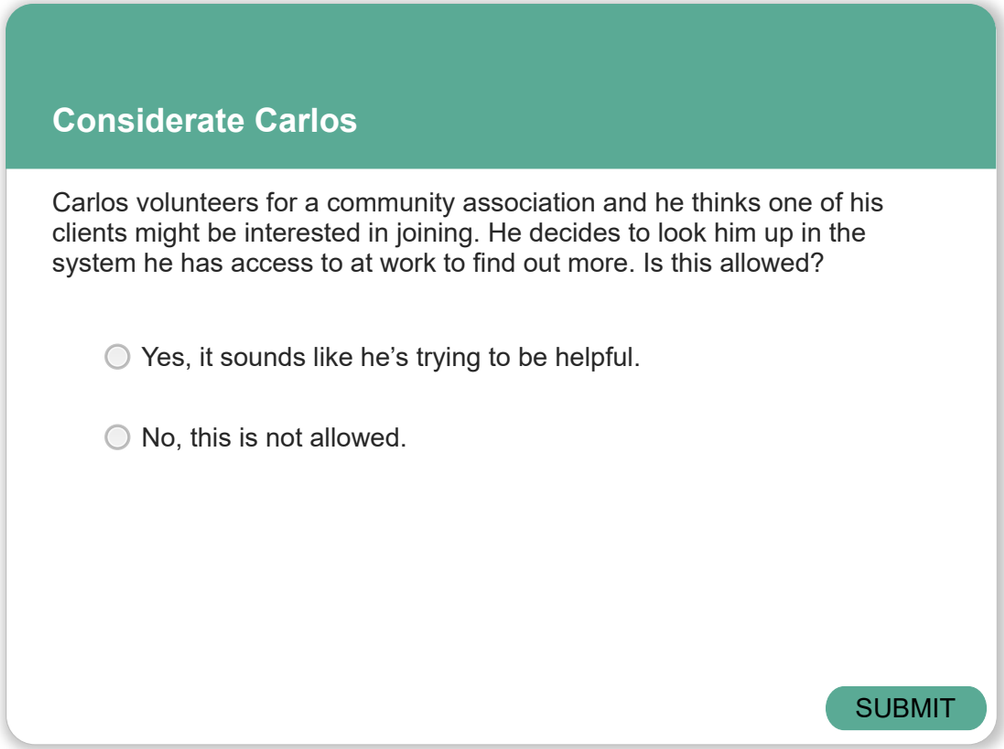
Notify your supervisor

Keep your supervisor informed of the incident. They can support you as you work with an investigator to respond to the incident.

Next steps

Once an information incident has been reported, the Privacy Officer will contact you to assess the incident and provide recommendations on the steps to take.
The investigator will work with you to:

- Report to the appropriate stakeholders
- Contain the incident and recover any information that was inappropriately disclosed
- Remediate including determining whether notifying impacted parties is necessary
- Create strategies to prevent a future incident (for example, privacy training).



DOWNLOAD CONSIDERATE CARLOS ACTIVITY DESCRIPTION

Information Sharing Agreements

Public bodies enter Information Sharing Agreements (ISAs) when there's a regular and systematic exchange of personal information between public sector organizations or between a public sector organization and an external agency. ISAs document the terms and conditions of the exchange of personal information in compliance with the provisions of the Act and any other applicable legislation. Contact RIS if you are considering entering into or initiating an ISA.

Privacy resources

There are privacy resources on the Energy Exchange, which will help you make informed decisions about handling personal information.

We encourage you to contact PrivacyOfficer@bc-er.ca if you have any questions.

CLOSE THIS TAB

Access to Information

Freedom of Information requests

In this section, we'll discuss access to information, and talk about both Freedom of Information — or "FOI" — and proactive disclosures of information outside of the FOI process.

The Freedom of Information and Protection of Privacy Act (FOIPPA) provides individuals a right to access their own personal information held by public bodies, as well as general information about government operations, programs and services – with limited exceptions.

The BCER is committed to expanding the public availability of government information and data through the disclosure of information without a formal FOI request. Whenever possible, information is released to the public as permitted or required by law.

Anyone can make an FOI request. We have a responsibility to be open, transparent and to provide people with the records to which they have a right of access. We receive FOI requests from a wide variety of applicants, such as: industry, individuals, political parties, the media, law firms, businesses, researchers, interest groups and other governments.

A person can ask for any record through FOI, but the request needs to be clear enough for an employee to identify the record. For the purpose of FOI, a record includes anything on which information is recorded or stored.

Access to information in a record is granted based on a line-by-line review, to ensure that the information is legally appropriate for release to the applicant that has asked for it, as permitted or required by law.

BCER employees have a “duty to assist” an applicant by taking all reasonable steps to respond quickly and accurately.

> **Duty to Assist:**
>
> Employees have a responsibility to be open and to connect people with the records to which they have a right of access, even if the request wasn’t necessarily worded clearly. You must look to fulfill the underlying intent of the request.

Records & Information Services (RIS) and you: a partnership

RIS is the centralized point of contact for processing BCER FOI requests. FOIPPA specialists administer the day-to-day work of providing timely responses to FOI requests received by the Regulator. The FOI team works with program areas to search and gather records. RIS works closely with you, because you are the subject matter expert on the records you work with. You know what information you hold, and whether the information is responsive to a FOI request.

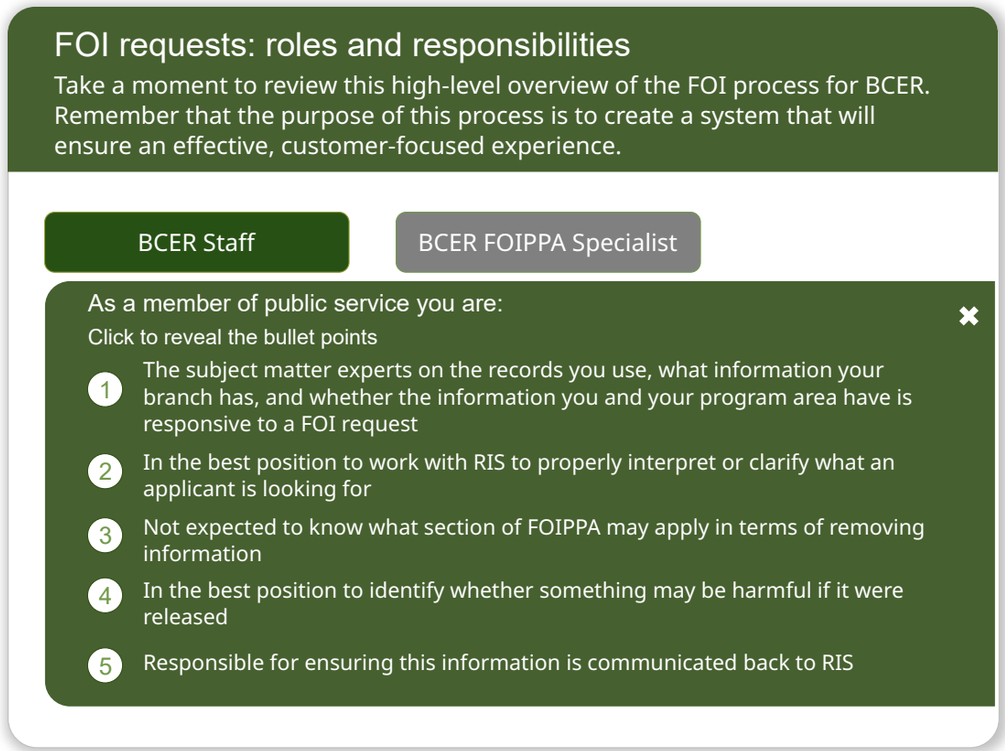
You are in the best position to identify whether something may be harmful if it were released — you’re not expected to know what section of FOIPPA may apply in terms of removing information. But you should let RIS know if you have additional information that may be relevant to the decision about whether information should be severed.

> **Severing Information:**

There are reasons the Regulator will remove – or 'sever' – information from a record prior to releasing it to an applicant.

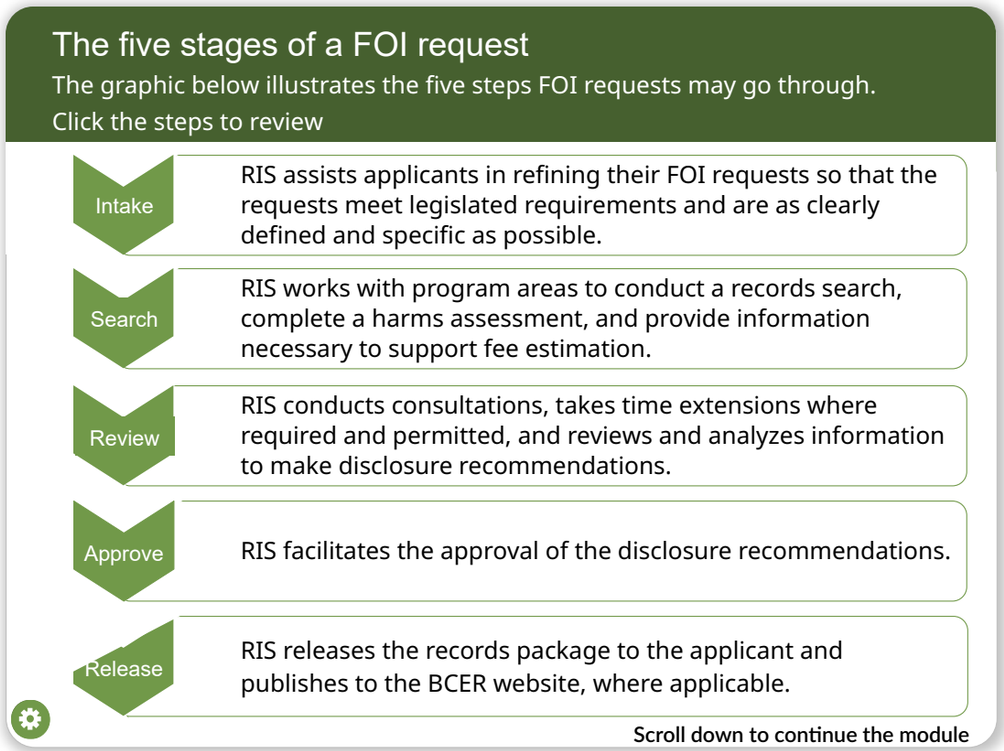
Ultimately, disclosure recommendations are made by the RIS FOIPPA Specialist and based, in part, on the context you provide regarding possible harms to government or third parties. A final decision with respect to disclosure, relying on RIS's recommendations and supported by your input, is made by the delegated head for the BCER.

The FOI team at the BCER are the experts when it comes to processing FOI requests. They have the expertise required to apply FOIPPA, to manage the legislated timelines, and to communicate with the applicant that made the FOI request. RIS also possesses the technology required to effectively sever information from records as required or permitted by FOIPPA.



It’s important to note that FOIPPA includes timelines for responding to FOI requests.

The five stages of an FOI request



Want to learn even more about the FOI process?

These links are recommended:

- FOI in the BCER
- BCER Internal FOI Process Flowchart
- FOIPPA Policy & Procedures Manual
- BCER – Freedom of Information

How to fulfill your duty to assist

BCER employees must make every reasonable effort to assist FOI applicants, and to respond to every FOI request openly, accurately, completely and without delay. After all, access to information is a foundational democratic principle.

The “duty to assist” goes beyond just meeting the letter of the law — it involves providing an excellent service experience to each applicant.

To meet your duty to assist an FOI applicant, you need to interpret FOI requests in the best interest of the applicant. This means steering clear of overly narrow interpretations, requesting clarification of requests when necessary and ensuring you’re being diligent in your search for responsive records.

To fufill your duty to assist:

- Adequately interpret FOI requests as a fair and rational person would expect – and in good faith
- Make a solid effort to discern the intent and goal of the requestor
- Conduct thorough searches for records (e.g. Outlook, Shared Drives, Teams, OneDrive, electronic systems, databases and any other office recordkeeping system) and document the search effort

FOI: The search process

A diligent search for records is one of the most important things you can do to assist people in accessing the information that they want. You are responsible for searching anywhere you have reason to believe recorded information might be stored that could be relevant to the request.

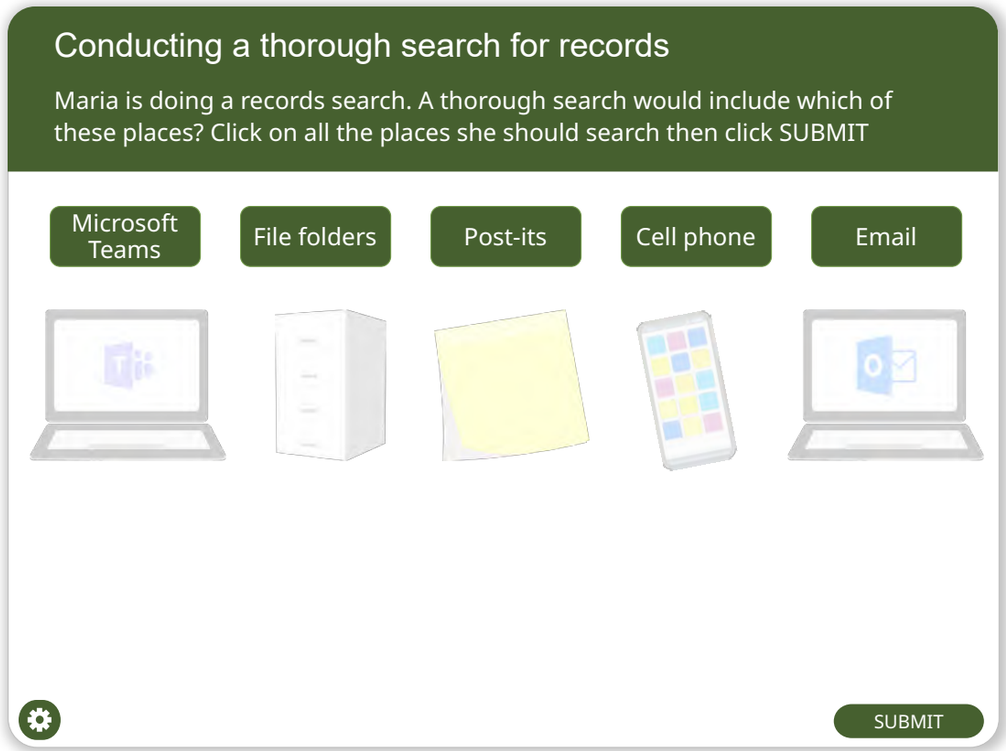
The BCER needs to provide evidence that a thorough and comprehensive search has been conducted. That’s why it’s very important that you document the details of your efforts, as well as an explanation in the event of a no-records response. Following good records management practices within your email and recordkeeping systems makes searching for records and responding to FOI requests much easier.

The search process must be thorough and widespread enough to ensure that all responsive records are located.

As we've already learned, emails are only one type of government records, and an adequate search for records that could be responsive to an FOI request requires more than just searching emails.

When conducting a search, you need to look in your office's electronic recordkeeping systems on Shared Drives, SharePoint sites and other collaboration tools, and in your paper or electronic notebook, as well any paper files.

The FOIPPA Specialist is your point of contact and will provide support to you to ensure you have a clear understanding of the request and what is required of you in responding.



To conduct a thorough email search:

- Search all Outlook items, not just your Inbox
- Search every mailbox you have access to, not just your own mailbox
- Search deleted, sent and subfolders
- Use broad search terms
- Use your expertise and knowledge on the topic to find everything that may be relevant
- Search common acronyms and synonyms

Also search for individual emails you may have printed or filed elsewhere.

If you have .PST files or have preserved emails in .PDF format to the hard drive of your computer or a Shared Drive, search these files if you have reason to believe relevant records may be saved there.

A note about archived emails:

If you have archived email files saved in a recordkeeping system, you may need to search those files as well. This is important to remember, because a search through your email account will not capture these files, which could contain records responsive to a request. This also applies to individual emails you may have saved elsewhere, outside of your email application.

PST files

PST files contain batches of Outlook content including emails, calendar events, tasks, etc. Folders, inboxes or entire mailboxes can be exported from Outlook in this format. PST files are not recommended for preservation purposes because they handle poorly in LANs, are easily corruptible, can't be searched in EDRMS environments, and can't be scanned for viruses. Contact the IT department at servicedesk@bc-er.ca for assistance with searching PST files.

Summary

It is also important to remember, that even transitory records need to be included if you have not yet disposed of them when the FOI request is received. You are not permitted to dispose of transitory records if they’re responsive to an ongoing FOI request.

Proactive disclosure

Proactive disclosure is the disclosure of information without the need for an FOI request. The BCER has a robust system that supports the proactive disclosure of information and discloses many kinds of data and information outside of the FOI process. Information is routinely released by responding to requests for information informally, as often as possible. In addition, the BCER website contains technical, spatial, analytical and other types of data and reports which are updated regularly, and available to the public.

The B.C. Data Catalogue also provides the easiest access to government's public data holdings, as well as applications and web services. Thousands of the datasets discoverable in the catalogue are available under the Open Government License — British Columbia.

We encourage you to contact FOIIntake@bc-er.ca if you have any questions.

CLOSE THIS TAB

FOIPPA Foundations

Privacy and Access Fundamentals

Overview

British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA) requires that public bodies, such as ministries, municipalities, and universities—along with public body contractors and service providers—protect all personal information they hold.

It's an important job!

Your responsibilities

As a public body employee, or service provider to a public body, you are required to protect personal information you handle in the course of your work. At the same time, you must make every reasonable effort to assist members of the public in their requests for information.

This course introduces the key ideas behind the Freedom of Information and Protection of Privacy Act (FOIPPA). By the end of it, you will be able to:

- Describe fundamentals of FOIPPA
- Describe your responsibilities under FOIPPA
- Describe how FOIPPA applies to your work
- Identify your privacy and access obligations

This course

The intended audience for this course is primarily B.C. public body employees and service providers to B.C. government. This course should take you about 60 to 90 minutes to complete. It consists of three modules:

Module 1: **The Basics**

Module 2: **Protection of Privacy**

Module 3: **Access to Information**

Each module also includes a Tip Sheet you can download to help you access and remember key information.

The exam

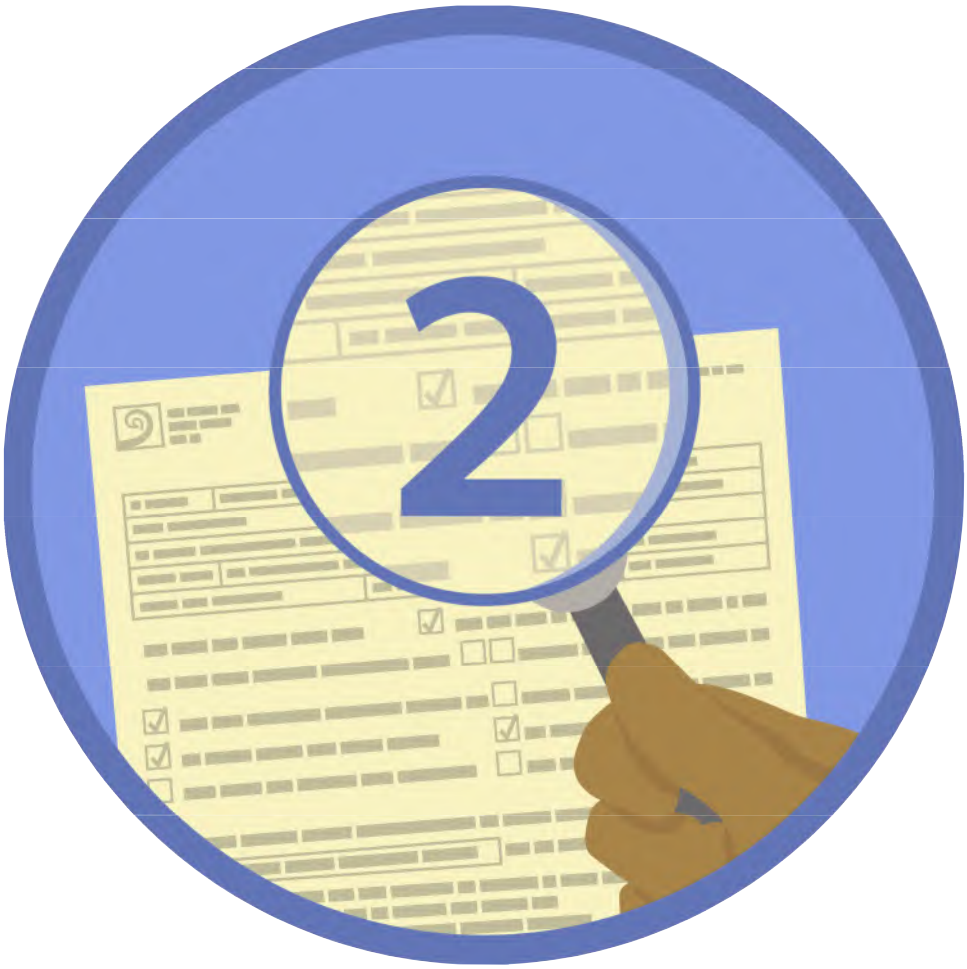
This course ends with a 10-question, multiple-choice exam to test your knowledge of key concepts from the course.

You will need to answer 80% of the questions correctly to pass. You may take the exam as many times as you like. As soon as you have passed the exam, you will be able to download a certificate of course completion.

Modules

Select a module below to get started:

1


2

We acknowledge all Indigenous peoples on whose territories we live, work, and play. We honour their connection to the land and respect the importance of the diverse teachings, traditions, and practices within these territories.

BRITISH COLUMBIA | Ministry of Citizens' Services

Module 1: **The Basics**

TIP SHEET

The Freedom of Information and Protection of Privacy Act (FOIPPA) is the privacy and access legislation that governs all public bodies in B.C. As a public body employee, contractor, or service provider, you must ensure that you manage information in accordance with FOIPPA.

Four domains of information management

Records management, access to information, privacy, and security all play an important role in the effective stewardship of information held by public bodies.

1. **Records management:** Records management is the system an organization uses to effectively capture and maintain information associated with business activities and transactions. Records include both print and digital records of such items as email, documents, maps, and handwritten notes.

2. **Access:** Public bodies are accountable to the public for ensuring access to records under the custody or control of the public body, with limited exceptions. This includes individuals' right of access to their personal information.

3. **Privacy:** Privacy is protected by public bodies treating personal information responsibly and lawfully. This includes ensuring personal information is collected, used, and disclosed appropriately.

4. **Security:** Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability of that information or system.

Where to go for help

- **Your supervisor** can help you determine when and how you are authorized to collect, use, and disclose personal information in the course of your work.
- **Your privacy officer** is the point of contact for privacy in your organization and can help you understand and resolve privacy issues, as well as navigate such processes as completing Privacy Impact Assessments.
- **Your FOI coordinator** is an expert in access to information and can help you navigate responding to FOI (access) requests.
- **The corporate privacy office** within the Ministry of Citizens' Services provides services to government and the broader public sector, including privacy training and resources such as the Privacy & Access Helpline.
- **The Office of the Information and Privacy Commissioner (OIPC)** provides independent oversight and enforcement of B.C.'s access and privacy laws, including the Freedom of Information and Protection of Privacy Act (FOIPPA). The office also has resources on privacy and access for public bodies, organizations, and individuals.

Custody and control

FOIPPA applies to all records in the custody or under the control of a public body, unless explicitly out of scope of the Act.

- **Custody** of a record means physically possessing that record. It normally includes responsibility for, access to, and security of, that record, as well as managing, maintaining, preserving, and disposing of it.
- **Control** of a record refers to the authority to make decisions about how a record ought to be managed throughout its lifecycle. If a public body has control of a record, even if it does not have custody of that record, the record still may be subject to FOIPPA. For example, a public body's records that rest with one of its service providers would be under its control but may not be in its custody.

Module 2:
Protection of Privacy
TIP SHEET

The Freedom of Information and Protection of Privacy Act (FOIPPA) works to protect personal privacy by preventing the unauthorized collection, use, or disclosure of personal information by public bodies.

Personal information

Personal information is recorded information about an identifiable individual other than their business contact information. It includes information about an individual's education history, employment history, health history, and even their personal opinions. It may also, depending on the circumstances, include other information, such as the person's name, home address, and DNA.

Questions to consider when handling personal information:

1. Why do I need the personal information?
2. Am I authorized to collect the information at this particular time (for example, is all of it directly related to and needed for the task at hand)?
3. What am I doing to protect the information I handle?
4. Am I using the information for a purpose consistent with why it was collected? If not, have I obtained **consent**?
5. Am I authorized to share the personal information?

Authorities

If a public body wants to collect, use, or disclose personal information, it needs to have an authority under FOIPPA to do so. These authorities outline the specific circumstances in which public bodies can **collect**, **use, and disclose** personal information.

As a public body employee or service provider to a public body, you may only access personal information that your public body has **collected in circumstances where it is required for your work and authorized under FOIPPA**. You may not access it for your own purposes.

TIP SHEET

Privacy tools

Privacy impact assessment (PIA)	**Helps identify possible impacts to individuals' privacy from new and existing initiatives**
Information sharing agreements (ISAs)	**Documents the terms and conditions of the exchange of personal information in compliance with legislation**
Information Sharing Code of Practice	**Supports responsible and lawful personal information sharing and the protection of personal information**
Privacy schedule in contracts for service providers	**Ensures service providers maintain the privacy standards for personal information set by FOIPPA**

Disclosing and storing sensitive personal information outside of Canada

A public body must complete a supplementary assessment for disclosures outside Canada when a program, project, or system includes *sensitive* personal information that is *stored* outside Canada. For more information, see **Guidance on Disclosures Outside of Canada**.

Information incidents/privacy breaches

An **information incident** is an event (or series of events) involving the collection, storage, access, use, disclosure, or disposal of confidential or personal information that threatens privacy or information security, and/or contravenes law or policy.

An information incident that threatens privacy is called a privacy breach and includes the theft or loss of personal information, or the collection, use, or disclosure of personal information that is not authorized by FOIPPA. A privacy breach may be accidental or deliberate.

There is a privacy breach notification requirement in FOIPPA. If there is a reasonable risk of significant harm to an individual as a result of a breach, the head of the public body must notify the affected individual and the Office of the Information and Privacy Commissioner (OIPC). Notification allows the individual affected by a privacy breach to take steps to mitigate possible harm.

Responding to an information incident/privacy breach

If you suspect an information incident/privacy breach has occurred, your first step is to immediately report the incident to the appropriate contact.

- **Public body employees** report to your supervisor, privacy officer, or other designated contact in your organization.
- **B.C. government employees, contractors or service providers** call 250 387-7000 or toll-free at 1-866-660-0811 (select option 3).

Once reported to the appropriate contact in your organization, they will help you through the remaining **steps to respond to the incident**.

In situations where containment of the information is possible (such as requesting an unintended recipient double-delete an email), consider making this request as soon as possible and advise the appropriate contact of steps taken.

Module 3:
Access to Information
TIP SHEET

Under the **Freedom of Information and Protection of Privacy Act (FOIPPA)**, individuals have a right to access:

- Their own personal information held by public bodies
- General information held by public bodies, including information about government operations, programs and services, with limited exceptions

Access to information is:

- A foundational democratic principle, supported by FOIPPA
- Permitted or required by law
- Granted based on a line-by-line review of the record to ensure that the information is legally appropriate for release to the person requesting it

Anyone, including individuals, political parties, media, law firms, businesses, researchers, interest groups, or other governments, may make an FOI request. An applicant may submit a request to access a record in any written format. If the applicant is making the request on behalf of another person, the applicant must also provide written permission from the other person (unless permitted by the **FOIPP Regulation**).

FOI exceptions to disclosure

While the public body's intention should always be to release information wherever possible, FOIPPA lists a number of **exceptions** to the release of information. These exceptions provide public bodies with the authority to sever (take out) information from a record before releasing it. The person who made the request retains the right to access the remainder of the record.

Mandatory exceptions	Discretionary exceptions
Public bodies **must** withhold information: • Subject to cabinet confidences • Harmful to the interests of an Indigenous people • Harmful to the business interests of a third party • Harmful to a third party's personal privacy	Public bodies **may** withhold information that is: • Subject to local public body confidences • Policy advice or recommendations • Legal advice • Harmful to: law enforcement; intergovernmental relations or negotiations; financial or economic interests of a public body; conservation of heritage sites; or, individual or public safety

In general, once a public body receives a request, the public body:

1. **Reviews the request** to clarify and/or determine if the information being requested is already available to the public
2. **Confirms receipt of the request.**
3. **Assigns a file number or method** of tracking the request.
4. **Establishes fees** to charge for the request (if any). Public bodies must not use fees to discourage an applicant from proceeding with a request.
5. **Searches for the record** anywhere there is reason to believe recorded information relevant to the request might be stored—and document the details of the search.
6. **Retrieves the record.**
7. Completes a **line-by-line review** of the information to determine what information (if any) may or must be severed before release. See **FOI Exceptions to Disclosure**.

   If some information must be severed, the public body must give the reasons, in writing, for refusing access to that information, as well as:

   - The FOIPPA provision(s) on which the refusal is based
   - Contact information for an employee who can answer the applicant's questions
   - Information about how to ask the Office of the Information and Privacy Commissioner to review the decision.
8. **Provides results to the applicant** within a maximum of 30 business days from the time the request was received.

Third parties: A public body may receive a request for access to a record that, although in the public body's custody, was either not authored by the public body or relates to a third party. If the public body thinks there may be harm in giving access to that information, it should consider whether they may or must consult with the third party before making a decision (**s. 23/24**).

Extensions: FOIPPA permits public bodies to take a 30-day extension for a number of reasons (**s. 10**). The Office of the Information and Privacy Commissioner (OIPC) may also authorize a public body to take an extension for periods longer than 30 days for the same reasons, or if the OIPC otherwise considers that it is fair and reasonable to do so.

Proactive disclosure: Public bodies are required to establish categories of records that are in their custody or control that are available to the public without an FOI request (**s. 70** and **71**) and to immediately disclose information where it relates to a risk of significant harm to people or the environment, or where disclosure is clearly in the public interest (**s. 25**).

Overview of the BCER's FOI Process

Information for the BCER's Internal FOI Review Group/Leadership

Prepared by:
Records & Information Services Branch – FOI Team

Updated: April 2023

FOI Request Processing – Typically 30 Business Days to…

1. Respond to an applicant (acknowledge/clarify request)
2. Notify appropriate staff/departments of new request
3. Search for/gather all responsive records
4. Combine and collate records into PDF format
5. Review records for responsiveness (relevance to request)
6. Review records for “harms” (line-by-line review) and withhold under appropriate sections of FOIPPA (“severing”; “redlining”; “redacting”)
7. Circulate draft release package for review by Leadership/SMEs – to identify missed harms and/or information that can safely be released
8. Circulate draft release package for review by Public Trust (Executive Director) and Legal Services for issues management/legal perspective
9. Complete any required edits (finalize the release package)
10. Obtain final sign-off by Delegated head
11. Release to applicant

FOIPPA's Exceptions to Disclosure…

The ***Freedom of Information & Protection of Privacy Act*** (FOIPPA) has mandatory and discretionary exceptions to disclosure:

- S.12 – Cabinet confidences
- S.13 – Policy advice or recommendations
- S.14 – Legal advice
- S.15 – Disclosure harmful to law enforcement
- S.16 – Disclosure harmful to intergovernmental relations or negotiations
- S.17 – Disclosure harmful to financial or economic interests of a public body
- S.18 – Disclosure harmful to the conservation of heritage sites, etc.
- S.18.1 – Disclosure harmful to interests of an Indigenous people
- S.19 – Disclosure harmful to individual or public safety
- S.20 – Information that will be published or released within 60 days
- S.21 – Disclosure harmful to business interests of a third party
- S.22 – Disclosure harmful to personal privacy

Current FOI Process

1. Formal written request is received from applicant (and logged)
2. Email notification of request/"call for records" is sent to program staff (those thought to hold records)
3. Responsive records are gathered by staff (or, in some cases, directly by FOI) and forwarded to Internal FOI for processing
4. Received records are collated/combined into single PDF
5. Records are reviewed by Internal FOI for responsiveness and "harms"; severing is applied pursuant to FOIPPA's exceptions to disclosure
6. Draft release package is circulated to internal FOI Review Group for feedback and VP approval ; Review Group always includes appropriate VP's, Legal Services and Public Trust
7. Release package is reviewed and signed off by Delegated head (EVP, PSTD)
8. Any required briefings are completed by Public Trust (e.g., to Executive, Ministry)
9. Records are released on-time to the applicant by FOI team
10. If publication criteria is met, copy of redacted request is published to the BCER's external corporate website

Two-Phased Approach to FOI Process Improvements

Phase 1 (Implemented)

- Establishment of an **internal FOI Review Group** to review/approve FOI release packages

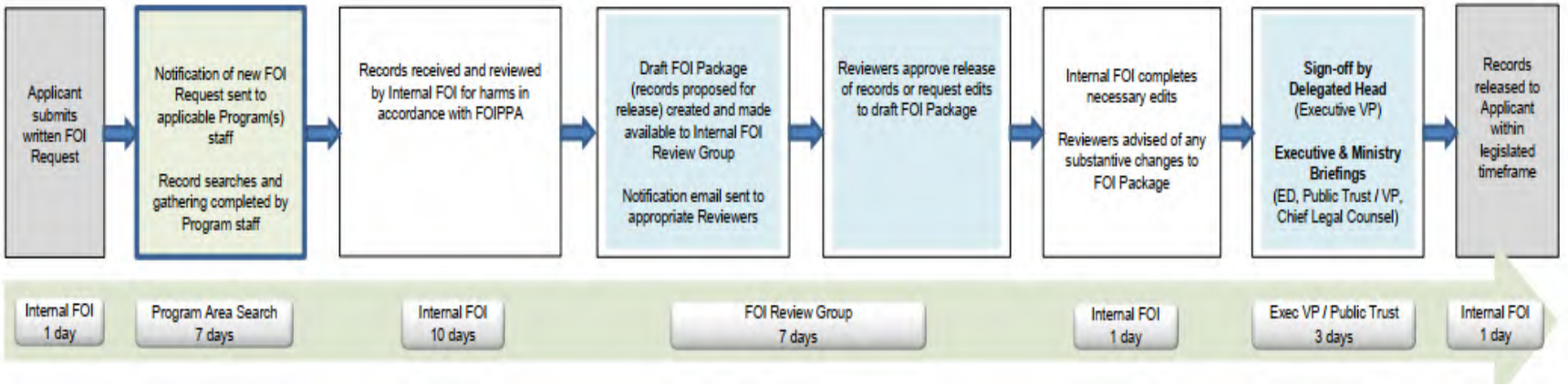
  Includes Leadership positions (VPs, EDs) (approvals received via email)

- Establishment of a formal **sign-off process** (Delegation matrix)

Phase 2 (To be implemented)

- Single point of contact model for FOI records searches
- Establish department (program) FOI contacts
- Contact receives notification emails of new FOI requests
- Contact coordinates records searches within their team
- Contact liaises with FOI and ensures responsive records are provided on time

FOI Process Flowchart



Phase 1 – Internal Review Group Implementation Benefits

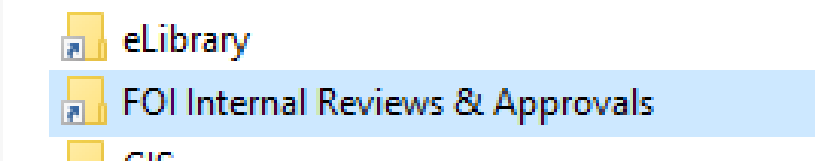
- Awareness of FOI requests relating to their areas
- "No surprises" – opportunity to review records and provide feedback prior to their release
- Reduced risk of sensitive information being released in error; or inappropriate withholding of information – programs know their business better than anyone
- Protects the Commissioner/BCER's reputation – shared accountability approach (FOI/SMEs); formal process in place

Review of FOI Release Packages

- Review Group is typically determined by program areas that have provided responsive records, with exception of Legal Services and Public Trust who review all requests
- If a request appears to have cross-organizational impact/interest, we'll notify all VPs and EDs as applicable of the request
- Release Packages relating to confidential personnel matters are sent to appropriate VP, Legal and Public Trust only for limited review

Review and Approval Process – How does this work?

- Folder has been created on the K: Drive for FOI Release Packages requiring review



- All Release Package(s) requiring review and approval are saved here (except confidential personnel-related packages)

- VPs and Program Leads have access to this folder and its documents

Review and Approval Process – How does this work (continued)?

- When a Release Package is ready for review and approval, a **notification email** from “FOI Intake” (FOIIntake@bc-er.ca) is sent to the appropriate Review Group members

- VPs and EDs have option to include their program leads/SMEs in the review process

- Public Trust and Legal Services are copied on the notification email

Example: Notification Email – "For Review and Comments"

What's Included in a FOI Release Package?

FOI Release Packages will include two items:

- **FOI Release Approval Form**
- **Redline** (records for release)

FOI Release Approval Form

The **FOI Release Approval Form** provides an overview of the Request and supports sign-off

- Date request received
- Legislated due date
- Applicant type (industry, media, individual, etc.)
- Request wording (“Any and all records relating to…”)
- Comments/background notes (e.g., summary of any severing applied)
- Description of any 3rd party consultations completed (names of parties, what pages they were consulted on, whether their concerns, if any, were addressed through severing)
- BCER’s recommendation on release – e.g., Full disclosure, Partial disclosure, Access Denied…
- BCER’s recommendation on publication (based on established policy/criteria)

“Redline” (Records for Release)

A **Redline** is a PDF (read-only) copy of all records deemed responsive to a request

- Pages may include red boxes around words, sentences or paragraphs
- This redlining is used to identify text deemed appropriate for redaction under FOIPPA; the FOIPPA section number that applies to the redaction is also visible

Example: "Redline"

S13

How Does the Internal Review Group approve an FOI Package?

- Simply reply to the original email that was sent by us (FOIIntake@bc-er.ca) with…
- "**Approved**" or "**No concerns**"
- Copy of "Approval" email is saved in official FOI processing file
- Delegated Head will **not** sign-off until all required approvals have been received

How Does the Internal Review Group Request Additional Severing, Ask Questions,

- Again, simply reply to the original email…
- If you think additional severing is required, please note in your reply the page number(s) and what text/info is harmful if released
- Please explain why - you don’t need to quote a section of FOIPPA, just provide us with a rationale
- We’ll try to support your severing requests, unless they’re indefensible under FOIPPA
- If unable to support, we’ll explain why not
- Any questions will be answered

Consultation Requests from Other Public Bodies (Informal Process)

- Sometimes we receive "**Requests for Consultation**" from other public bodies
- Where another public body has received a FOI request, and within their release package are copies of records created by/pertaining to the BCER (e.g. emails between BCER/Ministry staff)
- Standard process is to provide us with an opportunity to comment on disclosure (e.g. is any severing required, or no concerns with release?)

Different Process than FOI Requests (less formal/no sign-off):

- We email the records to appropriate staff for review/feedback (e.g. any harm with release?)
- Request details are provided: name of public body, request wording, applicant "type", deadline for our response
- We then inform the other public body of the BCER's views on disclosure – we ask to be informed if they're not going to support our recommendations

Internal FOI Team

Specialist, FOIPPA & Information Management:

- Dana Keough

Director, Records & Information Management:

- Mahia Frost

BC Oil & Gas COMMISSION

BC's *Freedom of Information and Protection of Privacy Act* (FOIPPA)

OVERVIEW

- FOIPPA applies to all public bodies in BC.
- The purpose of act is to make public bodies more accountable by;
  - giving the public the right of access to records;
  - Specifying limited exceptions to the right of access;
  - protecting personal privacy; and
  - Providing independent oversight by the Office of the information & privacy commissioner (OIPC) of any decisions made under the act
- The act applies to all records in the BC oil and gas commission's custody and under its control. The commission is responsible for the security and protection of these records.

What is a record?

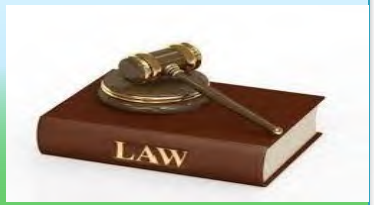
- A "record" is any information recorded or stored whether in electronic and hardcopy format.
- This includes:
  - oil & gas applications
  - Documents & reports
  - maps, drawings & photographs
  - Letters & written correspondence
  - emails
  - telephone records
  - note books, etc.

Duty to assist

When an FOI request is received by the commission, it has the duty to assist. This means the commission must:

- Make every reasonable effort to assist applicants;
- Respond openly, accurately and completely to requests within the 30 day timeline or limited extension period;
- Conduct an adequate search for records; and
- In limited circumstances, create a record where the data exists.

LEGISLATION



OIL & GAS ACTIVITIES ACT GENERAL REGULATION

- S. 17.1(c) – Applications and amendments for permits, including all submissions supporting the applications

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT EXCEPTIONS TO DISCLOSURE:

- S. 16 – disclosure harmful to intergovernmental relations or negotiations:
  - Negotiation & consultation with first nations in relation to specific applications;
  - All of the commission's communications with indigenous communities throughout the province;
  - Financial agreements & records of payments.
- S. 18 – disclosure harmful to the conservation of heritage sites:
  - Archaeology data;
  - Heritage sites.
- S. 22 – disclosure harmful to personal privacy:
  - Individual names, addresses, phone numbers
  - Consultation with landowners or other stakeholders

Commission privacy practices

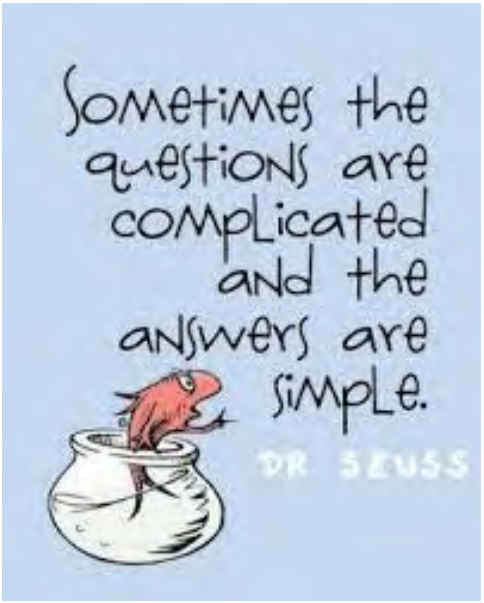
- All records are subject to FOI;
- Just because it is requested does not mean it will be released;
- The commission is committed to protecting personal privacy;
- The commission considers consultation and negotiation records with indigenous communities confidential and does not disclose these records to third parties;
- Only general information is publicly available on the commission's website such as BCOGC consultation areas, consultation and long term oil & gas agreements;
- The commission ensures it has measures in place to prevent the unauthorized collection, use and disclosure of personal and confidential information.

Helpful links

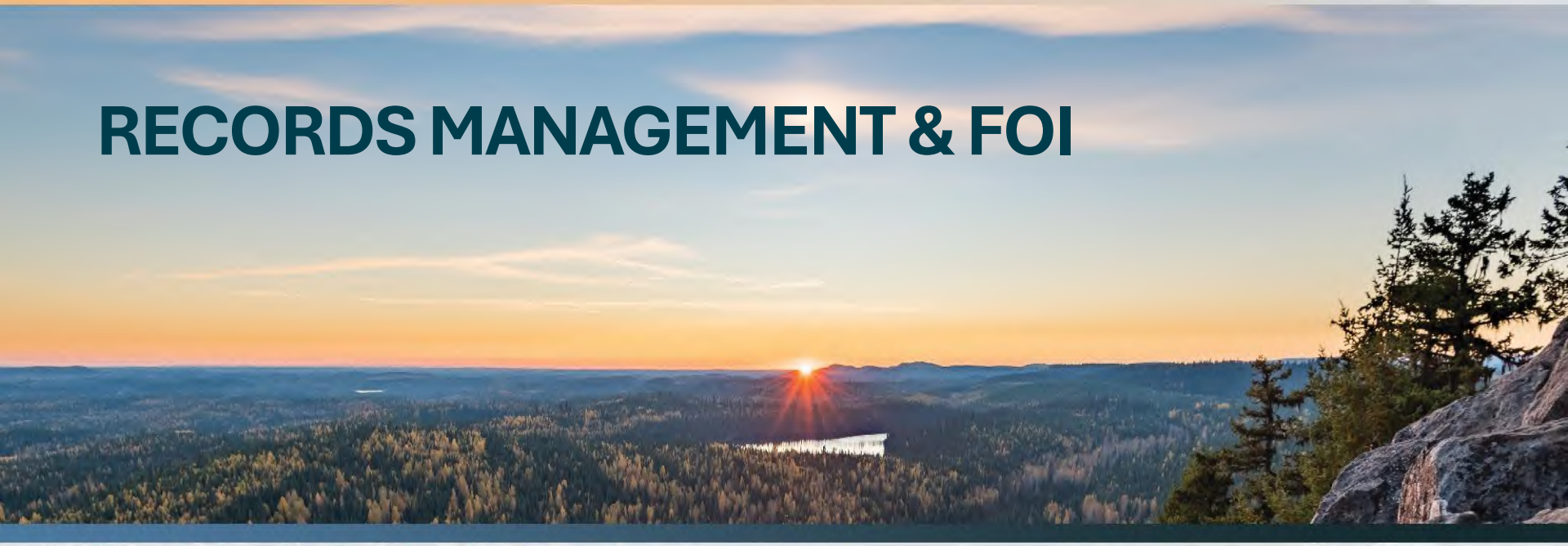
- Freedom of Information and Protection of Privacy Act
  - http://www.bclaws.ca/Recon/document/ID/freeside/96165_00

- Office of the information and privacy commissioner
  - https://www.oipc.bc.ca/

Any
Questions


Sometimes the questions are complicated and the answers are simple.
DR SEUSS

RECORDS MANAGEMENT & FOI



Records and Information Services (RIS)

Dana Keough and Mahia Frost

BRITISH COLUMBIA ENERGY REGULATOR

Records and Information Services

Our Role

EE Resources

Projects

Welcome to the Records and Information Services (RIS) space. The RIS team is responsible for Information Management (IM), Freedom of Information (FOI) and Protection of Privacy.

Our vision:

We have an information management program of excellence.

Our program enables the BC Energy Regulator to fulfill its mandate, facilitate legislative and policy compliance, provide good stewardship of our information, and support service delivery to citizens.

Our staff understand how we manage Regulator information, their responsibilities, and our processes.

Our mission:

We deliver an efficient and effective Information Management program and services to support the mandate of the BC Energy Regulator and its compliance requirements.

Information Management Resources

Freedom of Information (FOI) and Protection of Privacy

ORCS / Shared Drive Organization Projects / SharePoint

Information Management Act requirements

ARCS / ORCS – Records Classification systems

OGC Shared Drive Organization Projects

SharePoint Projects

Freedom of Information & Protection of Privacy Act (FOIPPA)

FOIPPA is provincial legislation that applies to all public bodies in BC.

The purpose of the Act is to make public bodies more accountable by:

- Giving the public the right of access to records;
- Specifying limited exceptions to disclosure;
- Protecting personal privacy;
- Preventing the unauthorized collection, use or disclosure of personal information; and
- Providing independent review of decisions made under the Act.

The Act applies to all records in the BCER's custody and under its control. The BCER is responsible for the security and protection of these records.

What is a Record?

A “record” is any information recorded or stored whether in electronic, hardcopy or other format.

Examples include:

- Oil & gas activity & application files (such as well, pipeline, facility (LNG), road, ancillary)
- Spatial data (GIS)
- Documents & reports
- Maps, drawings & photographs
- Letters & written correspondence
- Emails, messaging apps, text messages
- Telephone records
- Notebooks, handwritten notes, etc.

What is FOI-able?

- All BCER records, data and information fall within the scope of the Act and can be FOI'd
- Just because records are requested does not mean they will be disclosed.
- Confidential or sensitive information and data are protected from disclosure pursuant to applicable legislation and FOIPPA exceptions.
- Be aware that just because it's embarrassing does not mean it will be withheld or severed from responsive documents. Records can only be severed or withheld in accordance with the exceptions outlined in FOIPPA
- Disclosure should be the rule, not the exception
- If you are unsure, don't be afraid to ask questions!

BCER FOI Process

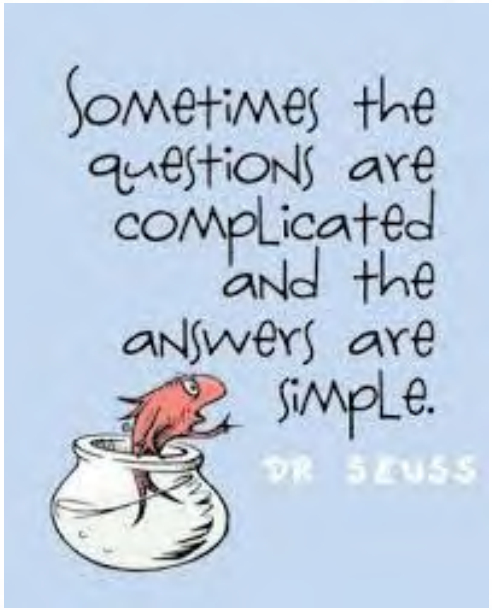
Where proactive disclosure is not possible, a formal written request is required:

- BCER receives FOI request and sends an acknowledgement letter to applicant and the 30-day timeline starts
- A call for records is sent out to program areas and responsive records are gathered
- Records are combined and collated into a PDF package
- A line-by-line review is conducted for harms and a redline package is created:
  - A redline is a PDF copy of all records deemed responsive to the request. Pages contains red boxes around sections that are recommended for redaction or severing of the information in accordance with FOIPPA.
  - This could include information where disclosure is harmful to law enforcement, business interests of a third party, personal privacy, conservation of heritage archaeology sites, or consultation with Indigenous peoples and landowners or other sections of the Act.
- Redline package is circulated for VP, SME, and legal review/sign off and approval
- Delegated head signs off
- Final severing/redactions are applied and a final release package is prepared and released to the applicant

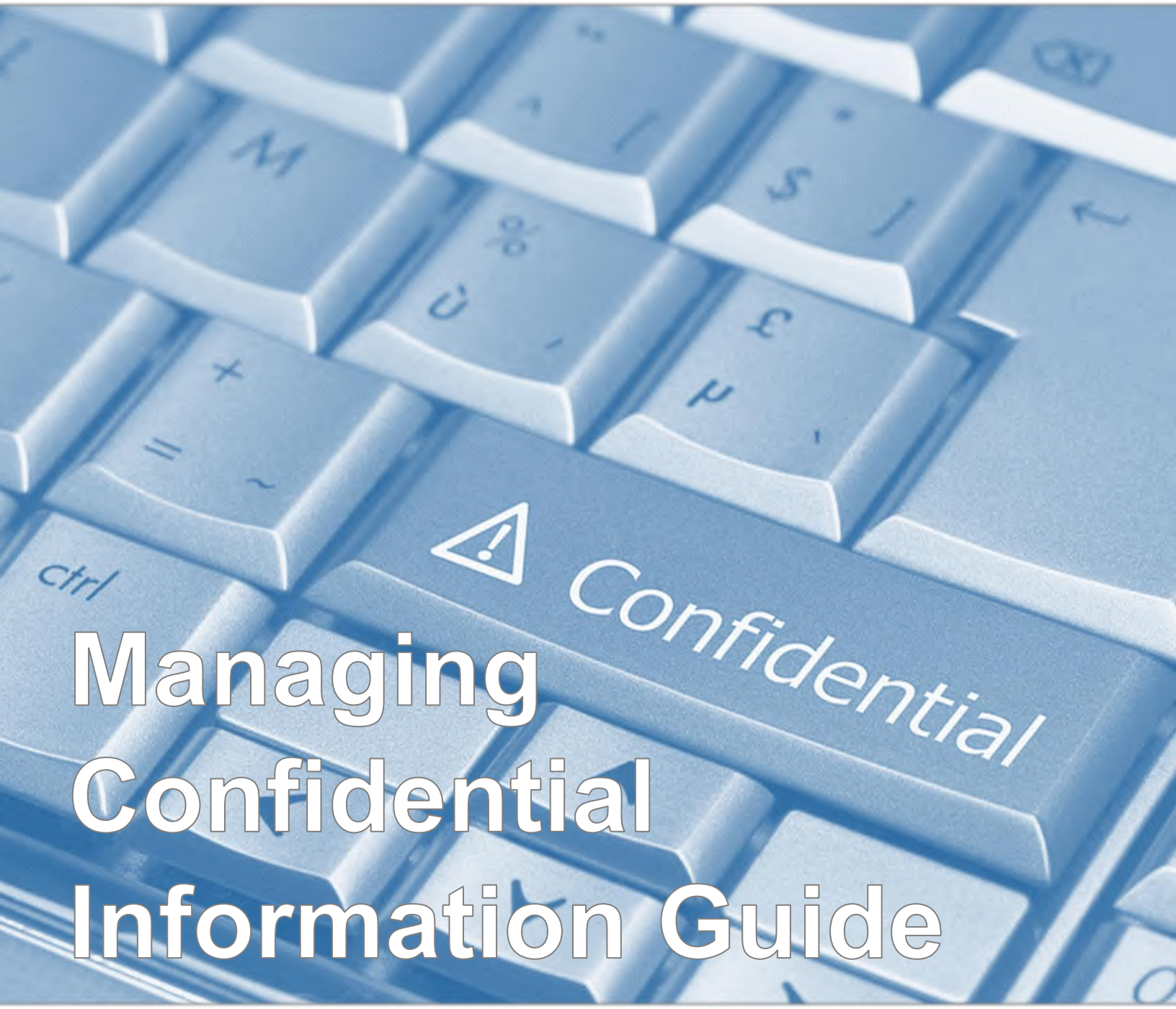
Tips for Good Privacy Practices

- Always be professional in your written communications
- When writing reports, state facts rather than personal opinions
- Use generalized terms/statements rather than directly identifying individuals, and limit personal information
- Have verbal conversations with colleagues to discuss facts prior to putting it in writing;
- Delete or destroy transitory records;
- Make time to delete and clean out your email accounts, including archives, deleted folder or other folders;
- Remove personal or junk emails;
- Review your communications prior to sending;
- Limit collection of personal information;
- Ensure good security measures are in place for the protection of sensitive and confidential information.

Any
Questions


Sometimes the questions are complicated and the answers are simple.
DR SEUSS

BRITISH COLUMBIA ENERGY REGULATOR



Managing Confidential Information Guide

June 2023

Table of Contents

Overview	3
Understanding Confidentiality	4
Basic Do's and Don'ts	5
In the Workplace	6
Outside the Workplace	7
Maintaining Confidentiality	8
Information Disposition	9
Pop Quiz!	10
Policies	12
Contacts	12

This guide is the result of collaboration between the Executive Vice Presidents and key staff from Legal Services; Public Trust; Information Systems and Technology; and Records and Information Services.

Overview

Information is one of an organization's most valuable assets. In the course of conducting business, BC Energy Regulator (BCER) employees often handle information that is sensitive due to confidentiality reasons or other obligations.

> Confidential information is information that, if compromised, could result in serious consequences for individuals, organizations, or government. Designating information as confidential depends on factors such as the value of the information, the source of the information, and the impacts of unauthorized use, disclosure, alteration, reproduction, loss or destruction.

All BCER employees (which includes all staff levels, contractors, and students working with the BCER) have a responsibility to appropriately manage and protect confidential information, regardless of whether they are the creator or recipient of the information. The public, industry, Indigenous communities and other government agencies regularly entrust the BCER with confidential information and rely on us to keep it safe while it is in our custody and control.

This guide has been created to assist BCER employees in securing:

- Our workplace.
- The information (sometimes referred to as data, documents, records, content) we create, receive and manage on behalf of the Province of British Columbia.

By consistently practicing a few simple habits, we can ensure confidential information is safeguarded.

Understanding Confidentiality

You may be unclear whether the information you have is confidential or not. The following questions are considered when assessing information for disclosure under the Freedom of Information and Protection of Privacy Act (FOIPPA) and may help you in determining confidentiality.

If the answer to any of these questions is yes, then the information may be confidential and require appropriate management. If you are unsure, discuss with your supervisor.

Does the information:

- Contain confidential consultation with other government bodies?
- Relate to economic policies/activities for which we are responsible? Or, contain a monetary value that is not public?
- Relate to administrative or personnel management plans that are not yet public?
- Contain information about a business's confidential negotiations with the BCER?
- Reveal a company's trade secrets?
- Contain legal advice or relate to a legal matter?
- Relate to records submitted, or prepared for submission, to Cabinet? Treasury Board?
- Contain policy advice prepared for the BCER or another public body?
- Consist of draft materials / advice / recommended courses of action?
- Have a legislative requirement concerning a period of confidentiality (such as well data)?
- Contain personal information relating to, about, or from individuals (e.g. personal opinions collected through a consultation process)?

More ways to look at it:

- Was the information supplied in confidence?
- Could release of the information harm a company's competitive position, result in the BCER no longer receiving the information, or result in undue financial losses or gains?
- Could release of the information harm our relationship with the Province, any of its agencies or other governments (i.e. other provinces, federal, indigenous, municipal, etc.)? Is the information ours to release (do we have the greater interest)? Or, could the timing of release have a negative impact on another public body or government?

Basic Do’s and Don’ts

- Remember your affirmation of the BCER’s **Employee Code of Conduct and Ethics**.
- Maintain a “clean desk” and always lock your computer (Windows Key + L) when you are away from your desk.
- Use the provided locked shredding bins whenever you are disposing of **transitory** confidential information (paper) in the office. Do not dispose of BCER information in recycling containers.
- Do not disclose BCER information, regardless of its sensitivity, without appropriate authorization.

- Use https://forgetmenot.bcogc.ca/ to store your BCER passwords. Do not write them down on sticky notes, store them under your keyboard, etc.
- Do not discuss or review confidential information in open work spaces, public areas, or when using public Wi-Fi.

Why this is Important

Protects the relationship of trust that is necessary for an effective working relationship between the BCER and our external partners (i.e. ministries, industry, educational institutions, Indigenous communities), and within our organization.

In the Workplace

Access

Security starts at the front door. Managing who gets into your workplace is an essential protection for confidential information. Follow these simple practices to prevent unauthorized access:

- If you see someone you do not know in your area or waiting at an access point, politely ask if you can help (if you are comfortable doing so).
- Do not let people follow you through access points if you do not know them.
- Report doors that do not close properly to your supervisor or Corporate Property and Administration.
- Ensure visitors to our workplace are signed in, and are accompanied by a BCER employee.

Your Workspace

Developing and implementing security-conscious work habits will reduce the likelihood of someone seeing or disclosing confidential information. Employees are expected to take reasonable steps to ensure the security of information they are creating or that is in their custody. Your practices should include:

- Locking your computer when you leave your desk to prevent unauthorized users from accessing the BCER's network and/or information.
- Securing sensitive documents in a locked drawer or cabinet.
- Maintaining a clean desk practice.

Clean Desk Practice

Remember to clear desks, workstations or work surfaces and secure all information prior to leaving the work area unattended:

- Clear your desks, workstations/surfaces, etc. of all confidential information at the end of each day, and secure the materials in provided storage spaces, or ensure your office door is locked.
- Take reasonable steps to safeguard BCER-issued IT assets and confidential information.
- Report any actual or suspected information security and/or privacy breaches immediately to your supervisor, the Director, Information Security (in the case of a data/network security breach), and the Director, Records & Information Management and Specialist, FOIPPA (BCER's designated Privacy Officers) if a breach relates to loss, theft or disclosure of personal information.

Outside the Workplace

Secure Remote Access Services (VPN) are provided by the BCER to ensure a secure connection to the network when working remotely. Once connected, you will be able to access the same network resources (e.g., shared drives) the way you normally would in a BCER office.

To ensure your information remains secure outside the workplace, take the following steps:

- Do not forward BCER information to personal accounts (e.g., Dropbox, Gmail, Google Drive, etc.).
    - Use only BCER-issued devices (laptops, smartphones, USB keys, etc.) for BCER work and for remote access to our network. BCER-issued devices offer security features, such as encryption, password protection, and the ability to be wiped remotely if lost or stolen.
- Do not use personal email or messaging (texting) accounts to carry out BCER business.
    - If this happens in an extenuating circumstance, you must copy the email(s) to your BCER email address or transcribe the text message into a document (e.g. word document), and delete the information from your personal account as soon as possible; ensure you share the least amount of information that is necessary in the circumstance.
- Avoid storing or transporting sensitive information on mobile devices. If an exception is required, please consult with your supervisor. Only use BCER-issued encrypted portable storage devices, and only as needed.
- In cases where mobile devices must be used to conduct BCER work, use strong passwords and do not share them with anyone else. Adopt good security practices for selecting passwords as outlined in the BCER's Information Security Policy.
- If you travel with physical documents, only take what is necessary for the job and make sure you have appropriate approval to transport the material.
- Protect confidential information while in transit or outside the office; do not leave mobile devices or confidential documents unattended or in plain view (for example, in the backseat of your car, etc.).
- When using remote access services, avoid public Wi-Fi and ensure you are the only one who works on your BCER-issued computer.
- Take appropriate measures to prevent others from overhearing or viewing confidential information, including ensuring your screen is not visible by others, preventing others from looking over your shoulder, and finding a private place to take a phone call.

Maintaining Confidentiality

The BCER aspires to uphold the highest standards in maintaining confidentiality and professional integrity.

Employees are required to affirm the **Employee Code of Conduct and Ethics** annually; it is a condition of employment. The Code of Conduct requires you to maintain the confidentiality of information or documents that come into your possession, or you have knowledge of in your role as a public servant. It also outlines the consequences of failing to do so. Please ensure you fully understand the responsibilities associated with maintaining confidentiality.

The requirement to comply with the BCER's Code of Conduct is a condition of employment. Please ensure you fully understand the responsibilities associated with maintaining confidentiality, as there are consequences of failing to do so. Possible consequences of non-compliance are outlined within the Code.

BC Energy Regulator's Employee Code of Conduct and Ethics:

Confidentiality

Confidential information, in any form, that employees receive through their employment must not be disclosed, released, or transmitted to anyone other than persons who are authorized to receive the information. Employees with care or control of personal or sensitive information, electronic media, or devices must handle and dispose of these appropriately. Employees who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing, releasing, or transmitting it.

The proper handling and protection of confidential information is applicable both within and outside of BCER and continues to apply after the employment relationship ends.

Confidential information that employees receive through their employment must not be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains.

Why this is Important

Protects the legal and business interests of the government and affected stakeholders.

Information Disposition

The same rules apply to confidential information.

BCER information, regardless of its format or sensitivity, must be disposed of in accordance with approved records retention and disposition schedules. These schedules are legal authorities that specify how long records are to be kept, and their final disposition (destruction or archival preservation).

Some information BCER employees create or receive may be considered transitory and should be handled accordingly. The following resources offer additional guidance:

- Transitory Records Guide
- Official vs. Transitory Records

Information that is subject to legal activity or requested under the Freedom of Information and Protection of Privacy Act (FOIPPA) cannot be disposed of until the matter has been resolved or the request completed. For more information on the types of information protected by FOIPPA, please contact one of the BCER's FOIPPA Specialists.

Why this is Important

Protects confidential or sensitive information that is often accessible to us as part of our work, and for which we are the trusted stewards.

Pop Quiz!

1. Which of these record types could contain confidential information?
   - ☐ Text messages
   - ☐ Draft briefing notes
   - ☐ Databases
   - ☐ Meeting handouts
   - ☐ Emails

2. Where should you dispose of transitory physical documents?
   - ☐ Recycling bins
   - ☐ Locked shredding bins

3. Should confidential information be disposed of when you are finished using it?
   - ☐ Yes
   - ☐ No
   - ☐ It depends

4. Is it okay to use your home email to do your work?
   - ☐ Yes
   - ☐ No
   - ☐ It depends

5. I work better with my coloured file folders holding my documents on my desk. Our office is secure, can't I just leave my stuff out and easy to find?
   - ☐ Yes
   - ☐ No
   - ☐ It depends

6. I am travelling between Kelowna and Fort St. John a lot these days. My personal USB device holds more documents than the BCER one – can't I just use that while doing this project?
   - ☐ Yes
   - ☐ No
   - ☐ It depends

Answers on the next page…

Pop Quiz Answer Key:

1. All of them! All of these records are considered government information, and any of them "could" contain confidential information. It doesn't matter what medium is used to produce a record, what makes it confidential is the context and the content.

2. In the locked shredding bins. BCER information should never be processed through recycling bins.

3. It depends. If the information is transitory then it may be shredded, or deleted, but if it's a record that you have used in making a decision, or if it records a working activity, then it must be managed according to the retention as outlined in our records classification systems. Please see our Official vs. Transitory records guide for clarity. And remember! Transitory information is subject to FOIPPA requests and may not be deleted if a request is open/active.

4. No. Do not use your home email to conduct BCER business. The BCER provides secure transmission and servers to protect the information we use to conduct our business.

5. Not if the information is confidential. Best practice recommends you clear your desk every evening, so you don't accidentally leave confidential material out.

6. No. The BCER issues encrypted USB drives for when you must carry documents on a portable storage device. If you are carrying BCER information, you must use a BCER-issued device. And remember to remove the records off the device and into the BCER storage environment when you aren't requiring mobile access!

Policies

- ✓ Building Access and Security policy
- ✓ Information Management Policy
- ✓ Information Security Policy
- ✓ Mobile Device Policy
- ✓ Use of IT Resources Policy
- ✓ Workplace Appropriate Use Policy

Contacts

If you would like more information regarding what is in this guide or wish to report an incident, please refer to the table below.

Commission Contact	When to Contact	Email
Corporate Property and Administration Corporate Property and Administration Resources	For general inquiries, or to report a facility or security breach.	servicedesk@bc-er.ca
Records and Information Services (Records Management) Information Management Resources	For general inquiries on how to manage government information.	servicedesk@bc-er.ca
Records and Information Services (FOIPPA and Privacy) FOIPPA and Protection of Privacy Resources	For general inquiries, or to report a privacy breach.	S17
IT Service Desk Service Desk	For technical support or ensuring your mobile device is encrypted.	servicedesk@bc-er.ca
Information Security/Cybersecurity Cybersecurity Resources	For general inquiries, or to report an incident of phishing, cybersecurity attacks, or a data/network breach.	servicedesk@bc-er.ca
Human Resources and Workplace Code of Conduct and Ethics Page	For general inquiries about the Code of Conduct and Ethics.	servicedesk@bc-er.ca

BC Oil & Gas COMMISSION

Managing Transitory Information Guide

Table of Contents

How can I identify Transitory Information? 3
What are my Transitory Information responsibilities? 4
Common categories of Transitory Information 5
1 Transitory messages 5
2 Transitory drafts 5
3 Rough notes and working materials 6
4 Transitory copies 6
5 Transitory systems information 7
6 Transitory Information from external sources 8
Examples of information that is NOT transitory 9
Contacts 10

This guide is based on the BC Government Transitory Information Guide.

Not all Commission information needs to be retained. This guide provides in-depth assistance to help you identify information that is transitory and understand the requirements of the Transitory Information Schedule. If all you need is the basics, refer to our Transitory Information Quick Tips Guide.

How can I identify Transitory Information?

Individual employees do not need formal authorization to destroy transitory information, so long as the records are not needed for a Freedom of Information (FOI) request or legal search, and the destruction is secure. However, employees sometimes do need help determining whether information is transitory or not.

There are a series of documents to help you understand what transitory information is:

- The Transitory Information Schedule defines and categorizes transitory information and establishes retention and disposition requirements for it.
- The Quick Tips Guide summarizes what is and is not transitory information.
- **This guide** provides an analysis and examples of transitory information categories, finishing with a table of examples of information that is NOT transitory.

Most transitory information is easy to identify because it has not been filed and is not needed for any reason. Some information is harder to assess, especially after relevant actions are completed. Content and context determine whether information is transitory, not its format or medium. If an email, handwritten note, draft, or copy is essential to understanding Commission business (e.g., how a decision was reached or program delivered), then the record must be kept, and is not transitory.

Records that are scheduled and classified by ARCS or ORCS and/or filed in the office recordkeeping system are never transitory. They need to be managed appropriately and securely destroyed in accordance with Commission requirements (see our Information Management Policy and the Documented Destruction Process Overview)

What are my Transitory Information responsibilities?

Both the Transitory Information Schedule and the Commission's Use of IT Resources Policy require employees to:

- dispose of transitory information that they are responsible for when it is no longer needed,
- ensure that the information is not relevant to a FOI request or request for legal discovery before proceeding with destruction, and
- always ensure that destruction occurs in a secure and confidential manner.

As an employee of the Commission, you need to be able to distinguish transitory information from records and data that document business decisions and actions. Routinely deleting transitory information ensures that the Commission is storing and managing the information it needs to keep.

Documenting Decisions

If your information contains evidence of actions or decisions, it must be managed as a record in the appropriate recordkeeping system. See Documenting Commission Decisions

Common categories of Transitory Information

Transitory Information includes, but is not limited to, records that are identified and described in the following common categories.

1 Transitory messages

Transitory messages are casual or non-substantive messages, in any format and including attachments, that are of only short-term use and are not needed to document an action or decision. They can take many forms (e.g., email, instant messages, chat messages in online collaboration tools, social media postings, facsimile [fax], voice/video message recordings).

Messages or attachments that are required for ongoing business needs are not transitory information. Due to their content or context, they must be retained (e.g., email documenting a policy decision, formal memo about Commission business, social media post that is the initial announcement of a new program). However, once these have been saved into an appropriate recordkeeping system, any additional copies of the messages may be considered transitory copies (see section 4).

Examples of transitory messages

- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- emails conveying an attachment (if it doesn't add value to the attachment)
- meeting arrangements
- routine correspondence about drafts and revisions
- requests to call someone

2 Transitory drafts

Transitory drafts are preliminary or incomplete drafts that do not contain significant annotations, comments, approvals, or substantial changes providing insight into the evolution of the final version. Once a subsequent draft or finished record has been developed and filed, these drafts are no longer needed.

Is this draft transitory or not?

- ☐ Is it complete/final?
- ☐ Is this the latest version available (i.e. it hasn't been replaced by a new version)?
- ☐ Was this draft used for formal consultation and review?
- ☐ Does it document a decision or approval?
- ☐ Does it represent a substantial revision?
- ☐ Is this draft subject to legislative, policy, or information schedule requirements?

If you answer "YES" to any of these questions, keep the draft, it is NOT transitory.

Examples of transitory drafts

- preliminary drafts that were never reviewed
- interim drafts that reflect minor editorial changes

3 Rough notes and working materials

Rough notes and working materials consist of preliminary, incomplete, or unused information maintained for the purposes of creating other documents, aiding memory, facilitating a routine action, or recording exploratory thoughts. They include documentation used to support projects and develop official records, often generated during brainstorming and collaboration activities.

Context and content affect the value of these records. If rough notes or other working materials help to illustrate a key decision-making process, particularly if the decision affected an individual, it is necessary to file and retain them (see CRO Directive 01-2019: Documenting Government decisions). Where subsequent or final records exist, however, the rough notes do not need to be kept, unless there is some other reason for doing so.

Examples of transitory rough notes and working materials

- outlines, calculations, summaries, flipcharts, and other rough notes not needed to support projects
- preliminary notes and working materials used to prepare a final record
- failed job output records resulting from abnormally ended jobs, programming errors, improper selection criteria, or unsuccessful data input

4 Transitory copies

Transitory copies are duplicates of existing records made for convenience or reference. These copies are not authoritative copies needed to replace originals as evidence of actions, decisions, or consultation. The following types of copies are transitory information:

a) Extra copies of records where the authoritative copy/original record has already been saved in an appropriate recordkeeping system. These include:
   - convenience copies
   - partial copies/extracts
   - copies made to support computer processing functions
   - copies used to support the development of other documents

b) Output from electronic systems created for reference purposes

c) Supplies of Commission publications and forms/templates (not including the official file copy of the publication/form/template or completed forms)

Copies kept for reference purposes may be classified under ARCS 358-20 Library/topical reference materials.

Examples of transitory copies

- copies created for convenience (e.g. agendas printed for use at a meeting)
- automatically generated copies of a master file that are no longer needed (e.g., processing/transmittal copies, user views that can be reconstituted)
- supplies not distributed (e.g., forms, pamphlets, newsletters, reports)

5 Transitory systems information

Transitory systems documentation consists of information of temporary usefulness generated for, or resulting from, computer systems operations (also known as transitory electronic data processing [EDP] records). It includes:

a) Input source documents used to enter information into a digital system (e.g., data entry forms), after which it is no longer needed
b) Automatically gathered/generated data processing information, including:
    - Data processing information generated in the process of transferring data between systems, obsolete after transfer is completed and validated
    - System output/reports generated for reference or for a client, not needed as part of a file or for system maintenance
    - Internet browsing documentation (e.g. browsing history, cookies, cache/temporary files)
c) Unneeded documentation of systems and internet usage.

Transitory systems documentation excludes data in the systems. Data that has been migrated or converted and thereby rendered redundant is covered by the Redundant Source Information Schedule, section 3.

NOTE: Systems documentation that is needed for operational purposes, ongoing maintenance, or for purposes of an investigation, is not transitory and should be retained in accordance with ARCS (see primaries 6450 Information System Development and Changes and 470 Security Management) or the appropriate ORCS.

Examples of transitory systems information

- data entry forms and EDP records not needed after the information is entered into a system
- internet browsing information (e.g., cookies, temporary internet files)
- data from connected devices that is not used, or is duplicated/ summarized in reports)
- empty folders and zero-byte files that have no further use
- notes, forms, and other input source documents used for data entry

6 Transitory Information from external sources

Transitory information from external sources includes solicited and unsolicited information from external sources that has been used solely for short-term reference purposes or not at all, including:

a) **Extracts or copies** of publications, promotional material, and other material from external sources.
b) **Unsolicited information** that is not used by the receiving office but may be redirected to the appropriate government body.
c) **Solicited and unsolicited information that is confidential in nature and is not needed to document a commission action or decision**.

NOTE: It is important to promptly and securely destroy or return any transitory information that contains personal or other confidential information that is not used by the receiving office, including:

- information identified as confidential in legislation or policy, as well as
- information that may not normally be recognized as confidential, except in relation to specific groups such as Indigenous communities.

The provision to securely return information to the sender has been included in the Transitory Information Schedule and in this guide to allow for this to happen when it is necessary and appropriate, in accordance with relevant legislation, policy, or the needs of the sender. (Please note that it is not the action of returning the information to the sender that renders it transitory. If a copy is needed for the Commission to take an action or make a decision, that copy should be retained in the appropriate recordkeeping system, even after the original is returned to the sender.)

Published items that are used as part of a procurement process or other transaction are **not** transitory.

Examples of Transitory Information from external sources

- advertising and promotional material not used for procurement or other transactions (e.g. spam, junk mail, catalogues, promotional DVDs, course announcements)
- newspapers or magazines used to compile news clippings relevant to a program area (the actual news clippings are filed under ARCS 295-04)
- unsolicited correspondence from the private sector that is not used for any actions or decisions
- information provided in confidence that is forwarded to the appropriate government body or returned to the sender, and not used by the Commission

Examples of information that is NOT transitory

Evidence

- drafts or revisions with information that is not documented elsewhere (e.g., directions to change a proposal or a course of action)
- draft legislation (file under ARCS 140-20)
- draft audit reports kept to comply with policy
- legal advice and agreements
- unread emails that are evidence of attempted consultation

Documenting Decisions & Actions

- business transactions documentation (initiation, authorization, or completion)
- records that include instructions, approvals and advice
- emails that document a policy, decision, significant action, or how a case was managed
- records that help explain the history of a relationship, decision or project

Operational Needs

- data that is needed for ongoing business
- information that is integral to a file about one event, client, or issue (i.e., a case file)
- reference material with ongoing value to the office
- work unit activities documentation (e.g. work schedules, assignments)

Official Communications

- formal communication about Commission business
- social media post officially announcing a new Commission program

Official/Final Records

- final reports and recommendations
- official copies of agendas and minutes
- official copies of policies, directives, procedures, standards, guides
- signed briefing notes

DO NOT destroy any transitory information that:

- may be relevant to a current/anticipated FOI request or legal discovery, or
- is stored in backup systems, which are an essential part of protecting the Commission's information assets (i.e. "triple deleting" is not allowed).

Policies

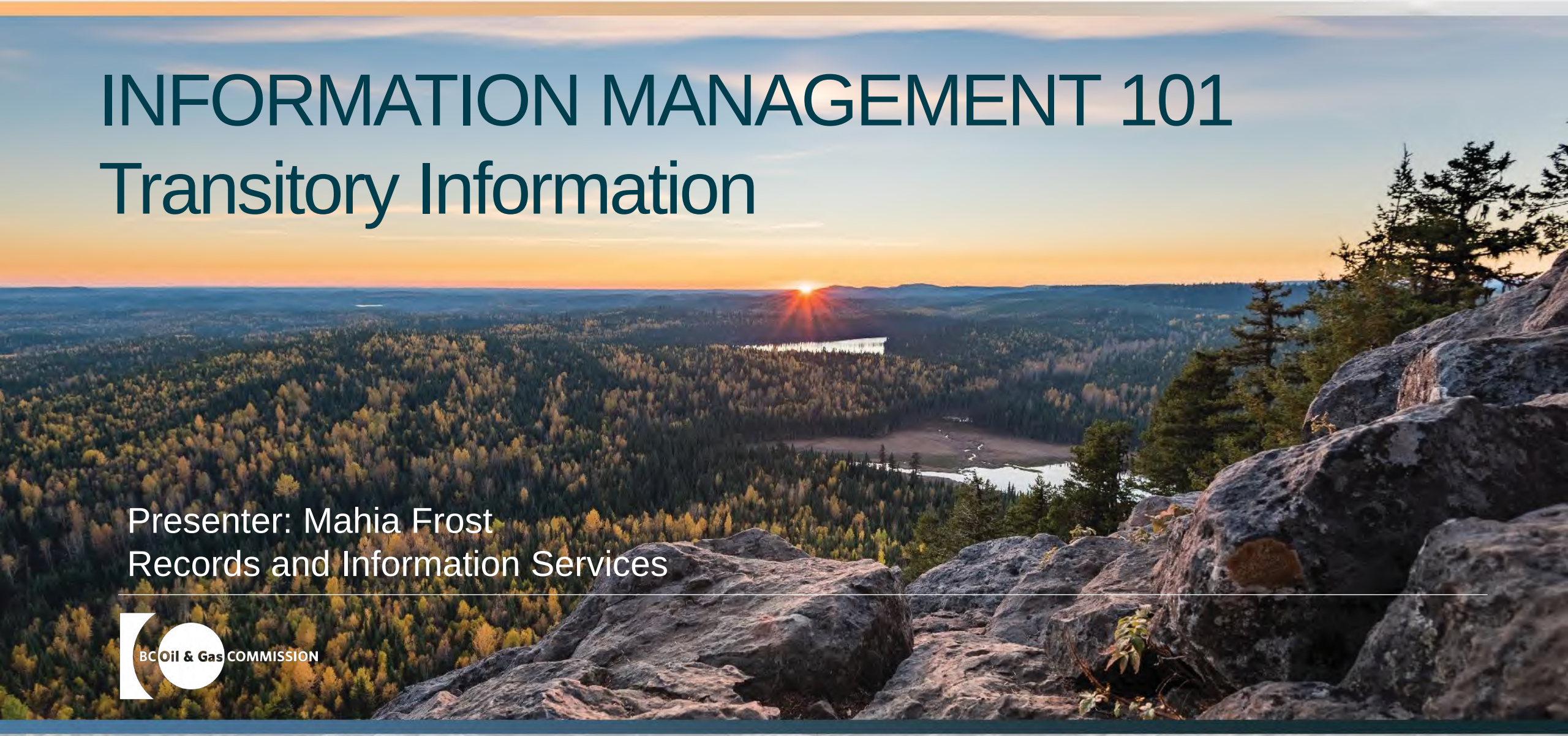
- ✓ Employee Code of Conduct and Ethics
- ✓ Information Management Policy
- ✓ Use of IT Resources Policy

Contacts

If you would like more information regarding what is in this guide or wish to report an incident, please refer to the table below.

Commission Contact	When to Contact	Email
Records and Information Services (Records Management) OGC Information Management Page	For general inquiries on how to manage commission information.	servicedesk@bcogc.ca
IT Service Desk Service Desk	For technical support.	servicedesk@bcogc.ca

INFORMATION MANAGEMENT 101
Transitory Information



Presenter: Mahia Frost
Records and Information Services

BC Oil & Gas COMMISSION

Objective

For you to gain a better understanding of transitory information, and why this is an essential element in managing BCER information.

IM Framework in BCER

Information Management Act

Freedom of Information and Protection of Privacy Act

Professional Governance Act

Information Management Policy

Documenting Government Decisions Directive

ARCS/ORCS/Transitory Information Schedule

Legislation and Policy

Definition – Record

INTERPRETATION ACT
[RSBC 1996] CHAPTER 238

"record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise;

Transitory Information

1. Transitory messages
2. Transitory drafts
3. Rough notes and working materials
4. Transitory copies
5. Transitory systems information
6. Transitory information from external sources

All quite common sense – records of low value and temporary usefulness

Category 1: Transitory messages

Messages and attachments that do not document a business activity or decision (i.e., message content lacks substance).

- Correspondence about meetings
- Announcement of a social event
- “cc” and “FYI” messages (unless you are the main staff member responsible for the matter)
- Routine message about drafts and revisions
- Emails conveying an attachment (if it doesn’t add value to the attachment)

Category 2: Transitory drafts

Drafts with no significant annotations, comments, approvals, or substantial changes; i.e. preliminary drafts that were never reviewed or interim drafts that reflect minor editorial changes

Is this draft transitory or not?

- Is it complete/final?
- Is this the latest version available (i.e., it hasn't been replaced by a new version)?
- Was this draft used for formal consultation and review?
- Does it document a decision or approval?
- Does it represent a substantial revision?
- Is this draft subject to legislative, policy, or information schedule requirements?

If you answer "YES" to any of these questions, keep the draft, it is NOT transitory.

Category 3: Rough notes and working materials

Information used to support projects and develop official records.

- Flipchart pages (and other brainstorming records)
- Outlines, calculations, summaries, and other rough notes not needed to support projects
- List of ideas or suggestions
- Preliminary notes and working materials used to prepare a final record

Category 4: Transitory copies

Copies not needed as evidence of decisions, actions, or consultation.

- Extra copies of records where the official copy/original record has already been saved in an appropriate recordkeeping system.
- Output from electronic systems created for reference purposes
- Copies created for convenience (e.g. agendas printed for use at a meeting)
- Supplies not distributed (e.g., forms, pamphlets, newsletters, reports)
- Partial copy / extracts

Category 5: Transitory systems information

Information that is no longer needed after it is entered into systems or generated as output.

Unneeded systems and internet usage documentation.

- Internet browsing information (e.g., cookies, temporary internet files)
- Data input forms
- System output created for reference or for providing to clients

Category 6: Transitory information from external sources

Published, solicited and unsolicited items that have been only used for reference, referred to another office, or returned to sender

- Advertising in various formats
- Newspapers and magazines
- Spam or junk mail
- Unsolicited correspondence not used for any actions or decisions
- Information redirected to the appropriate office (such as a forwarded email)
- Confidential information returned to sender (unless used by the BCER to take an action or make a decision)

Summary of Transitory Information

- Common sense rules
- You, as the expert in your work, can make the decision
- You can delete when your use is complete
- Clears the way to focus on managing the records that have value.

Important Caveat

Do not destroy transitory information that may be relevant to a Freedom of Information (FOI) request or legal discovery.

What is not transitory

Consider if the record is:

- Required to document a decision
- Required to meet legal or financial obligations
- Needed to sustain BCER operations, programs, or administration
- Integral to a case (i.e., needed as context for related records)
- Needed for accountability purposes
- Covered by ARCS or ORCS

If you answer “YES” to any of these questions, the record is NOT transitory.

Examples of what is NOT transitory

These are official records and should be filed into the recordkeeping system.

Evidence

- drafts or revisions with information that is not documented elsewhere (e.g., directions to change a proposal or a course of action)
- draft legislation (file under ARCS 140-20)
- draft audit reports kept to comply with policy
- legal advice and agreements
- unread emails that are evidence of attempted consultation

Documenting Decisions & Actions

- business transactions documentation (initiation, authorization, or completion)
- records that include instructions, approvals and advice
- emails that document a policy, decision, significant action, or how a case was managed
- records that help explain the history of a relationship, decision or project

Operational Needs

- data that is needed for ongoing business
- information that is integral to a file about one event, client, or issue (i.e., a case file)
- reference material with ongoing value to the office
- work unit activities documentation (e.g. work schedules, assignments)

Official Communications

- formal communication about Commission business
- social media post officially announcing a new Commission program

Official/Final Records

- final reports and recommendations
- official copies of agendas and minutes
- official copies of policies, directives, procedures, standards, guides
- signed briefing notes

Recordkeeping systems in the BCER

Structured shared drives, (with the *Administrative Records Classification System* (ARCS) and *Operational Records Classification Systems* (ORCS) applied)

Properly configured **SharePoint sites**, with ARCS and ORCS applied

Line of business applications (e.g., case management systems such as AMS and IRIS)

Hardcopy (paper) filing systems

Tools

Email clean up tools in Outlook

Assign policy tool in Outlook

A few email principles

Tools – Managing Email Guide

Deleting Email Appropriately

Now that you know what constitutes an official email record and how to save them properly, you should delete the redundant (duplicate) emails from your Outlook. You are also encouraged to delete transitory emails, personal emails and other non-record reference material that is taking up valuable space.

Deleting emails quickly and appropriately ensures that your inbox will remain clean and clutter-free.

This section will provide guidance on simple Outlook tools that will help you to delete your emails appropriately. It will also include simple exercises you can perform to find and delete common categories of transitory email.

Tools include:

- **Clean-up Tool**
- **Auto-delete Folders**
- **Assign Policy for transitory emails**
- **Empty Deleted Items on Exit**
- **Exercise: Find and Delete Emails to Distribution Lists**
- **Exercise: Find and Delete Meeting Requests**

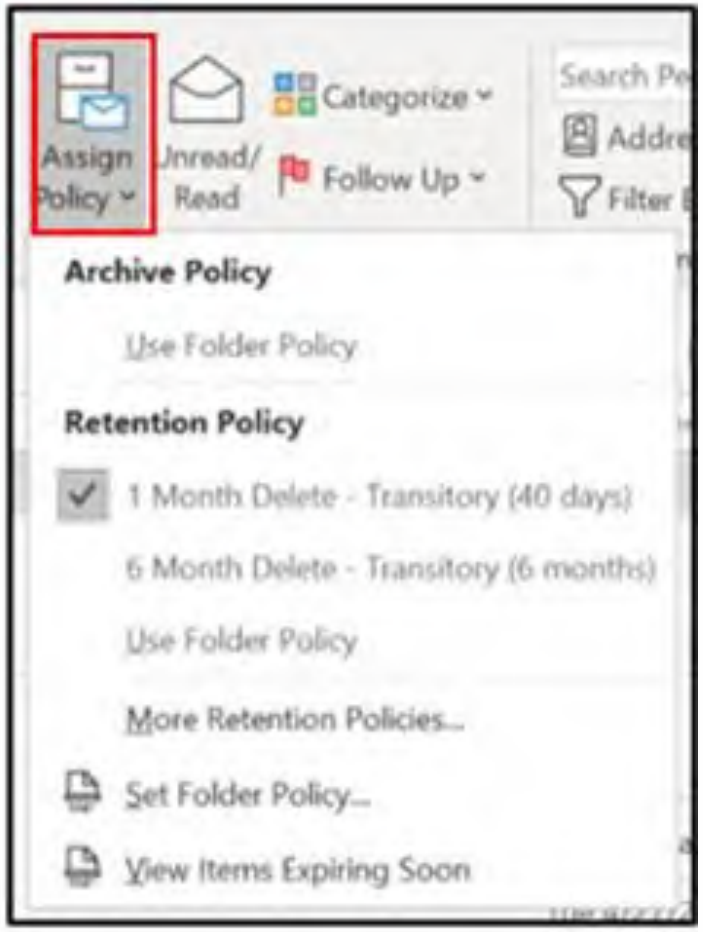
NOTE: You are prohibited at all times from 'triple-deleting' emails (i.e. attempting to purge an email from your 'Recover Deleted Items' folder).

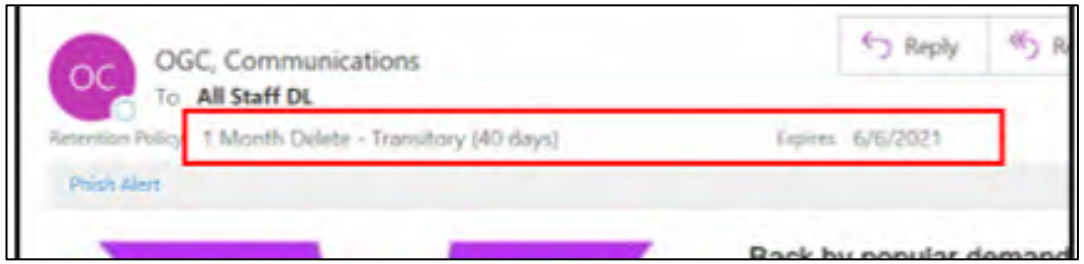
This should not be confused with double deletion, which happens when deleted emails are cleared from the 'Deleted Items' folder. The double deletion process is important for clearing space in your Outlook account but must only be done if the items in question are permitted to be disposed of.

Assign Policy in Outlook

To apply the policy directly to an email:

1. Select the transitory email and click on the Assign Policy button.
2. Choose the retention you prefer for the email from the picklist.
3. Notice the email now states your chosen retention period, with the “expires” (deletion) date. When the email reaches the expiry date it will be automatically deleted and moved to your Deleted Items folder.





Governing Principles – Emails.

- The email sender (initiator) is responsible for saving internal email
- The principal receiver is responsible for saving external email
- Working groups should assign responsibility for shared mailboxes

Bonus good practice tips:

- Empty Deleted Items on exit from Outlook
- Working groups determine who is capturing the official record for a file

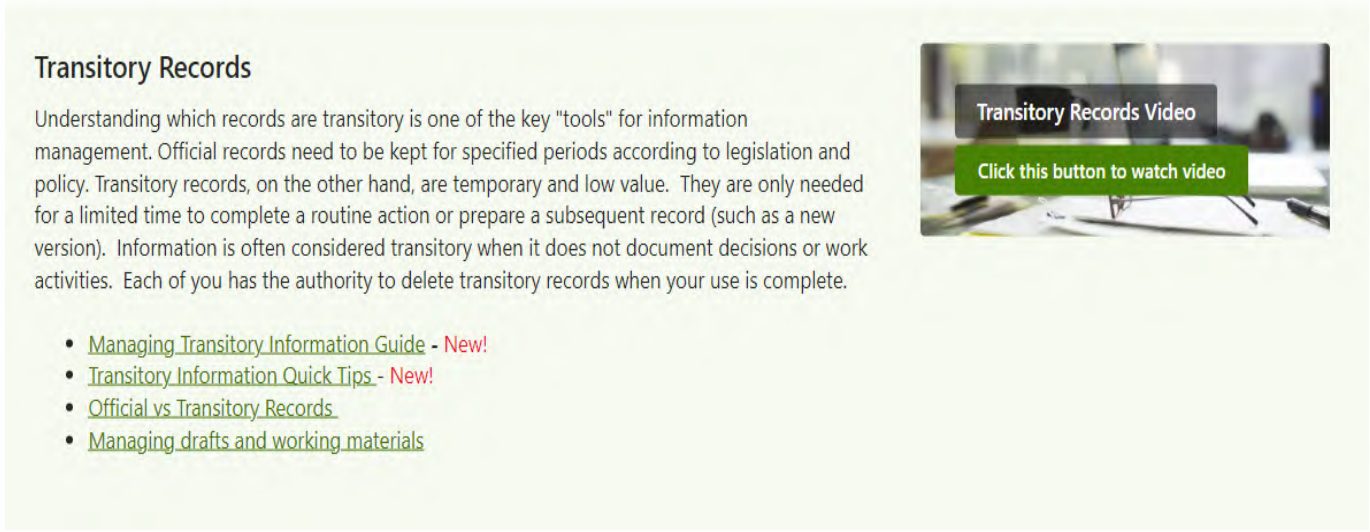
Resources

[Information Management on the Energy Exchange]

[Transitory Information Video]

[Email Management in an FOI World video]

[Documenting Decisions Training video]



Questions?

SCRIPT: MODULE ONE, MANAGING EMAIL IN AN FOI WORLD

Hello from your Records & Information Services Branch! Today we are talking about email management in the context of Freedom of Information or, as we more commonly say, the FOI world. Email management is a challenge that we all take different approaches to. Some of today's tips may already be part of your daily habits, but with so much of our business being conducted through email, we thought a refresher would be helpful.

We are focusing on the connection between Freedom of Information and emails because the Commission receives a significant number of FOI requests - an average of 60 a year. Depending on the topic, requests for information can involve many staff and program areas through the Commission, and an FOI request often includes all related email communications.

To begin our conversation about email management, let's review some best practices for emails in an FOI world.

First, remember to keep communications professional, not personal. Emails requested under FOI cannot be altered, so when you write an email always think: would you feel comfortable seeing this in a newspaper article? Would you mind your supervisor or our executive reading this? If in doubt, then don't write it down. . . Remember, "embarrassment" is not an exception to disclosure under the Freedom of Information and Protection of Privacy Act!

Another best practice is to keep your emails limited to one topic. Trying to cover several topics in one email can be a problem for a couple of reasons – first, it can be unclear where to file your email in the recordkeeping system (such as in Kermit, or on the shared drive). Second, it can cause us to provide extra and unnecessary information in response to an FOI request. Unrelated information cannot be removed or redacted from a record unless one of the sections of the Act applies. Just because the information doesn't relate to the topic doesn't mean it's automatically out of scope. Limiting your email to one topic makes it easier to manage as a record, and supports a 'tidier' response for FOI.

So, now that we're creating great email communications… how can we make searching for them in Outlook easier? Well first, know what you can get rid of on a daily basis – what we call your transitory material. Also know what is non-transitory and needs to be kept as an official record, to document or support the work you are conducting for the Commission.

Transitory records are records of temporary usefulness – they're only needed for a limited period of time to complete an action, or to prepare a final record.

The most common email examples are personal messages, announcements of social events, meeting arrangements, and copies received for convenience or reference – unless you are the person responsible for that matter!

Another transitory email is an email that is part of a "string". When you are having a back and forth email conversation, the **final** email, which contains *all* of the back and forth emails, is the official record

of the conversation, and all of the emails leading up to that can be considered transitory, and deleted from your Outlook.

Another example is if you have filed the email into the recordkeeping system, such as in AMS or KERMIT, the email left in your Outlook is now considered redundant. It's a duplicate, and can be deleted.

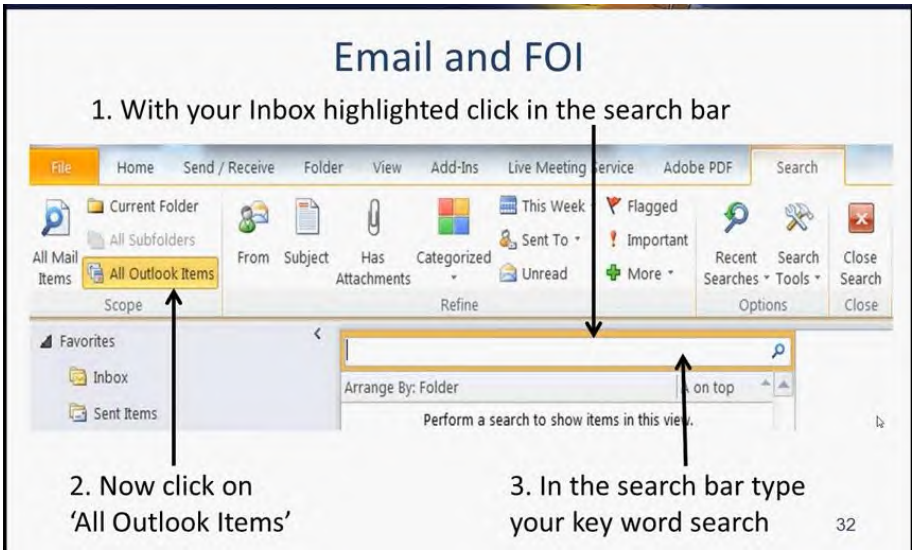
The value of knowing what is transitory is that you can delete those emails when you are done with them. By doing so, you keep your Outlook more manageable, and you're not having to sift through unnecessary records. You can find what you need faster, and easier. It also prevents transitory emails from being included in FOI requests… remember that a request for emails under FOI isn't just limited to the emails in your inbox. It includes your sent items, your deleted items, and anything in your sub-folders.

To end this module, I'd like to share a final tip to help you find all of the relevant emails in Outlook when doing an FOI search (or a search for emails under litigation). If you conduct your search in the order as follows, you should get complete results – this is what's known in the FOI and litigation worlds as 'adequacy of search' and it's what we are aiming for!

First, with your inbox highlighted, click in the search bar.

Now, click on 'All Outlook Items'.

Then, in the search bar, type your key word search.



Today we've covered some key information about email in the context of FOI requests. To summarize, there are a few things we can do to make email management and the FOI search process a little easier:

1. Keep your Outlook tidy – delete transitory items promptly

2. Keep emails to a single topic, and professional
3. Know your proper search methods

We have guides for email management and understanding what is a transitory record on our new intranet section on MyOGC, so please check those out for more information. Thank you and stay tuned for more informational videos!

SCRIPT: MODULE TWO, TRANSITORY RECORDS

Hello everyone, in this video I'd like to talk about transitory records - how to recognize them, and how to manage them**.**

As you may know, we have a few "rules" when it comes to managing Commission records. Official records need to be kept for specified periods according to legislation and policy. Transitory records, on the other hand, are records of temporary usefulness that we only need to keep for a limited period to complete a routine action or prepare a final record *(word bubbles saying "notes that are transcribed into a system" "do you have time to meet today?" "draft # 3, grammar fixes") .* The basic principle is information is considered transitory when it does not document decisions or work activities.

Who can decide if a record fits the transitory criteria? You can! Using your good judgement, when you are finished using the record, you can simply destroy it.

First, how do we recognize a transitory record?

We will start with the obvious categories, such as announcements of social events, personal messages or advertising material.

Then there are transitory records of short-term use, such as:

- Copies created for convenience or reference.
- Duplicates, partial copies or extracts, which you are no longer referencing.
- Input source documents, which are no longer required because the information from them is in the official system.
- Meeting arrangements.
- A simple message saying something like "can you call me this afternoon".
- And Cc copies on emails– unless you are the key staff member for that matter.

Finally, there are records related to drafts and working materials. Drafts, and routine correspondence about revisions, can be transitory. Working materials, such as outlines, calculations, preliminary notes and other rough content that you use to prepare a final record, can be transitory. However, if a draft, email, or other record is <u>essential to understanding Commission business</u>, such as how you reached a particular decision, then the record is not transitory and must be kept. Working materials relating to the preparation of legislation, regulation, or audit reports must also be kept. Outside of these, you can discard those seven versions that provide no information on decisions or approvals once you have a complete and final document.

SCRIPT: MODULE TWO, TRANSITORY RECORDS

Each Commission employee has the authority to identify a transitory record, so **you** can determine whether a record is, or is not, transitory.

So, how do we manage transitory records?

By promptly destroying them. This helps us to better identify and file official records into our recordkeeping systems, where we can find them more easily. It keeps our email accounts clear of unnecessary clutter. The Commission avoids unnecessary costs for storing and processing transitory records, and it supports the Freedom of Information, or 'FOI', process (*see our video "Email Management in an FOI World" for more information on that!).*

There is one important exception related to destroying transitory records - if we receive an FOI or litigation search request, we must provide all relevant records, including any transitory information that exists at the time of the request. Transitory information that is subject to such requests must be held pending completion of the applicable FOI response process and review period or the applicable litigation activities. *(word bubble: "Do NOT destroy any transitory information relevant to a FOIPPA request or legal discovery!")*

So now you know how to identify transitory records, and how to manage them. We have some great reference guides on MyOGC such as "official vs. transitory records", "email decision diagrams", and "managing drafts and working materials". And as always, get in touch with your friendly records folks for more information.

Thanks for your time!

Practical Guidance for the BC Energy Regulator's Board of Directors

Legislative Requirements relating to Board Communications (Email) and Records

Introduction

The Regulator is an open and transparent crown corporation that is subject to legislative requirements relating to information access and records. As an agent of government, the Board and each Director are governed by applicable policies, directives and legislation relating to the public's right of access to information under BC's Freedom of Information and Protection of Privacy Act (FIPPA) and the retention of non-transitory records (i.e., records of decisions) pursuant to the Information Management Act (IMA) and the duty to document key activities and decisions.

In the course of their Board-related duties, Directors may exchange communications and documents (records) with other Directors, employees of the Regulator, and third parties using personal email accounts. Such exchanges of information fall under the control of the Regulator making them subject to FIPPA and the IMA, so it is important to manage these records appropriately. The following information has been prepared to support Directors in understanding and meeting their legislated responsibilities in relation to these Acts.

Records and Information Management

Definitions:

Term	Description
Government record	All recorded information created or received by government bodies while conducting business activities and maintained as evidence of those activities, regardless of their digital or physical format. Under the Interpretation Act, a record includes "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise."
Transitory records	Records of temporary usefulness that are not required to support or document the Regulator's business or decision-making activities. As with all records, they can exist in any format or medium (e.g., paper or electronic). Transitory records can be deleted or destroyed when no longer needed for reference purposes. Examples of transitory records include:

	• Emails, correspondence and attachments that do not document a business activity or decision (i.e., message content lacks substance). • Drafts of documents with no significant annotations, comments, approvals, or substantial changes. • Reference copies (e.g., for meetings) not needed as evidence of decisions, actions, or consultation. • Rough notes and working materials. • Published or unsolicited information from external sources (e.g., advertisements, newspapers, magazines, spam, junk mail, unsolicited correspondence not used for any business decisions or actions). IMPORTANT: Transitory records cannot be destroyed if an FOI request has been received or eDiscovery initiated, and the records relate to the topic or specified date range.
Non-transitory (Official) records	It is important to understand which records are not transitory. Non-transitory (official) records need to be filed in an appropriate recordkeeping system (e.g., a secure system maintained by the BCER's Corporate Governance branch). If any of the criteria below applies to a record, the information is NOT transitory and should be kept: • Record supports or provides evidence of a key decision (i.e., of the Board) • Record is required to meet legal or financial obligations • Record is needed to sustain the Regulator's operations, programs or administration • Record is integral to a case (i.e., needed as context for related records in a case file) • Record is needed for accountability purposes
Custody (of a record)	Having physical possession of a record, even if a public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.
Control (of a record)	Having the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure.

Director Responsibilities under the IMA:

Use of Personal Email

- Directors use personal email accounts to exchange information with other board members, employees of the Regulator or third parties.
- Emails related to the business of the Regulator's Board should be kept separate from other types of communications; it may be helpful to:
  - save them in a separate folder; and
  - include a standardized subject line in emails to make them easily identifiable and searchable (e.g., BCER: Q2 Financial Statements).

- Transitory emails should be routinely deleted when no longer required for reference. This should include deleting them from both the "inbox" and "deleted items" (trash) folders.
- Transitory records that have not been deleted could be subject to an FOI request or eDiscovery. These records cannot be legally destroyed if an FOI request has been received or eDiscovery initiated and the transitory records relate to the requested information.

Duty to Document

- The Regulator must follow government's "duty to document" directive and maintain adequate records of decisions which includes Board records. Refer to government's video on Documenting Government Decisions for more information about this requirement.
- The Board Secretary maintains official records of the Board on behalf of the Regulator.
- If a Director creates or receives a communication (e.g. from another Director or third party) that supports board business or provides evidence of board decision-making, a copy of the email and any attachments should be forwarded to the Board Secretary for filing as such records are not in the Regulator's custody (and thereby inaccessible) but are under its "control".

Access to Information / Freedom of Information

Definitions:

Term	Description
Freedom of Information (FOI) Request	An FOI request is a formal process to ask for information that falls under the custody or control of a provincial public body. A request must be made in writing and typically relates to specific information held by a public body about an individual (their personal information) or pertaining to its business activities and mandate.
Exceptions to Disclosure	FIPPA establishes an applicant's right to access records held by a public body, however there are certain exceptions to accessing records. Not all requested information is deemed appropriate for public release. Some exceptions to disclosure are mandatory (information that meets the criteria must be protected), while others are applied to requested information at a public body's discretion.

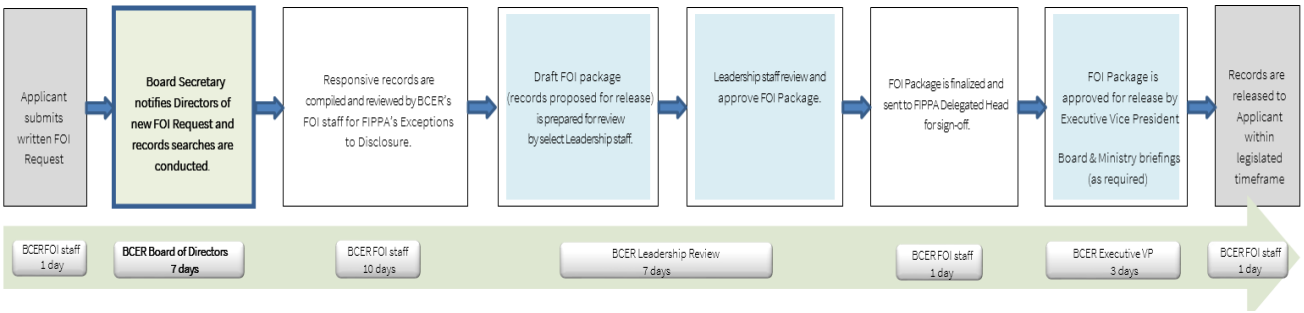
Director Responsibilities under FIPPA:

Responding to an FOI Request

- FOI requests typically follow a 30-business day processing timeline.
- When the Regulator receives an FOI request, a formal process is followed:
  1. The first step involves interpretation of the request (i.e., understanding what information an applicant is seeking) and identifying all locations where responsive records may reside.
  2. If responsive records could reasonably include communications held by Directors in their personal email accounts, the Board Secretary will send a "Call for Records" to each Director on behalf of the Regulator's FOI staff.
  3. The Call for Records is an email that includes the wording of the request, the applicant "type" (e.g., media, law firm, etc.) and any pertinent details to support the search for records.
  4. Directors will be requested to provide the Board Secretary with copies of records, should they exist, that they believe may be responsive to the request.

- An FOI request does not automatically result in the release of information; a line-by-line review of each responsive record in an FOI package is completed by the Regulator's FOI staff to identify information that should be fully or partially withheld (protected) under FIPPA's exceptions to disclosure.
- Prior to any release of information, FOI packages are reviewed by select members of the Leadership group.
- Once all Leadership feedback and approvals have been received, an FOI package is signed off by the Executive Vice President, People, Strategy & Transformation (FIPPA Delegated Head); the Board may be briefed on a request as appropriate.
- Records are then released to the applicant within the legislated timeframe for response.

FOI Request Process Flowchart



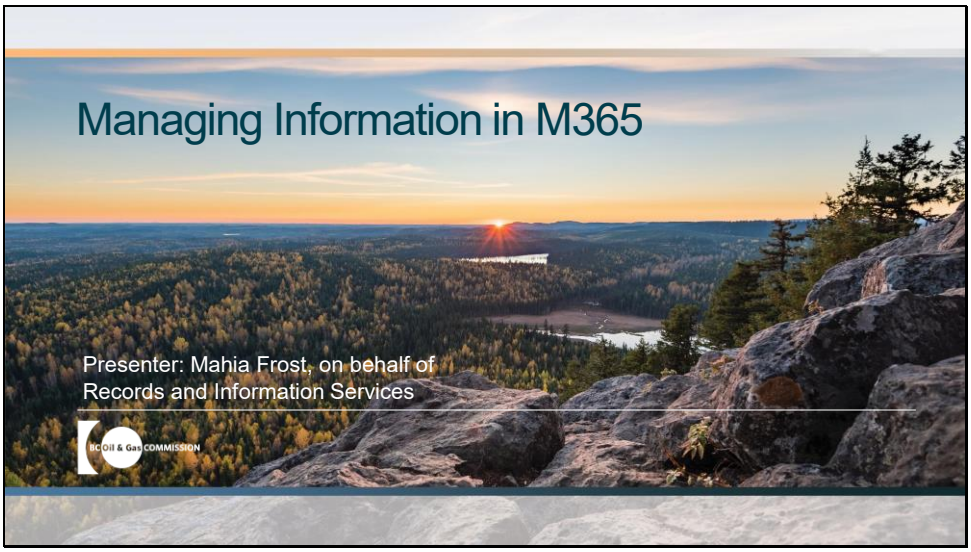
FIPPA's Exceptions to Disclosure

Section	FIPPA Section Title	Description of Exceptions to Disclosure	Application
12	Disclosure Harmful to Cabinet Confidences	Information that would reveal Cabinet confidences (e.g., advice, recommendations, policy considerations, legislation or regulations submitted or prepared for submission).	Mandatory
13	Disclosure Harmful to Policy Advice, Recommendations or Draft Regulations	Information that would reveal advice or recommendations. This section is intended to allow for full and frank discussion of policy issues during deliberative processes.	Discretionary
14	Disclosure Harmful to Legal Advice	Communications between a public body and its legal counsel to protect solicitor-client privilege.	Discretionary
15	Disclosure Harmful to Law Enforcement	Information that could harm a law enforcement matter.	Discretionary
16	Disclosure Harmful to Intergovernmental Relations or Negotiations	Covers matters that could harm the relations between BC levels of government and governments from other provinces and jurisdictions (e.g., Government of Canada, council of municipality, regional district board, aboriginal government, government of a foreign state, international organization of states).	Discretionary
17	Disclosure Harmful to Financial or Economic Harm	Information which could cause financial or economic harm to a public body or to the government.	Discretionary

18	Disclosure Harmful to Conservation of Heritage Sites	Information about heritage sites which would result in the exploitation or destruction of those sites.	Discretionary
18.1	Disclosure Harmful to Interests of an Indigenous People	Information that could reasonably be expected to harm the rights of an Indigenous People to maintain, control, protect or develop their cultural heritage, traditional knowledge, traditional cultural expressions, or manifestations of sciences, technologies, or cultures.	Mandatory
19	Disclosure Harmful to Individual or Public Safety	Information that could result in harm to any person's mental, physical, or emotional health or to public safety.	Discretionary
20	Information that will be Published or Released within 60 Days	A public body may withhold information from an applicant if it is already for sale to the public, or if the public body plans to release or publish the information within 60 days.	Discretionary
21	Disclosure Harmful to Third Party Business Interests	Public bodies are often in possession of commercial or financial information related to outside businesses and must withhold that information from an applicant if release would cause harm to the business. A three-part test must be met for a public body to appropriately apply section 21.	Mandatory
22	Disclosure Harmful to Personal Privacy	Personally identifiable information must be protected. Except in limited circumstances, a public body must not release an individual's personal information without their explicit consent.	Mandatory

Additional Resources (available soon on the Board Portal)

- Video: Transitory Records
- Video: Email Management in an FOI World

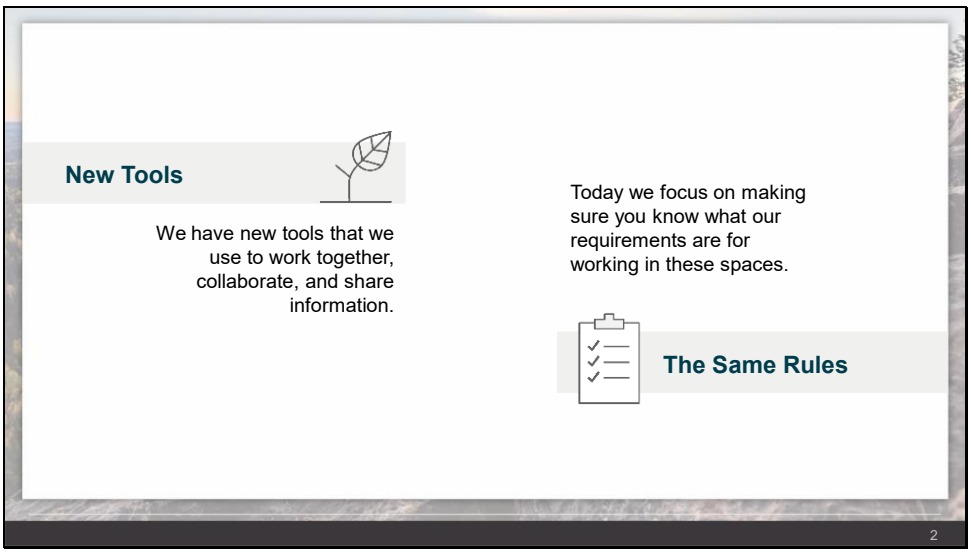


Hello, and welcome.

My name is Mahia Frost, and I am presenting on behalf of the Records and Information Services Branch. We are the team that supports Commission staff on how to manage our information according to best practice and legislation.

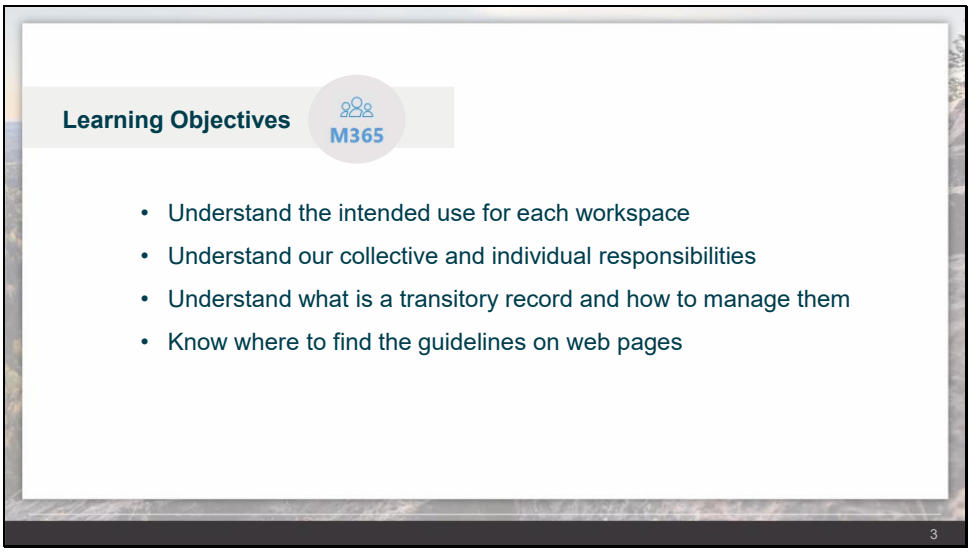
I would to acknowledge that we are honoured to be living and working on the traditional territory of the Lekwangan speaking people.

Today we are going to talk about managing information in the new technological environment, Microsoft 365.



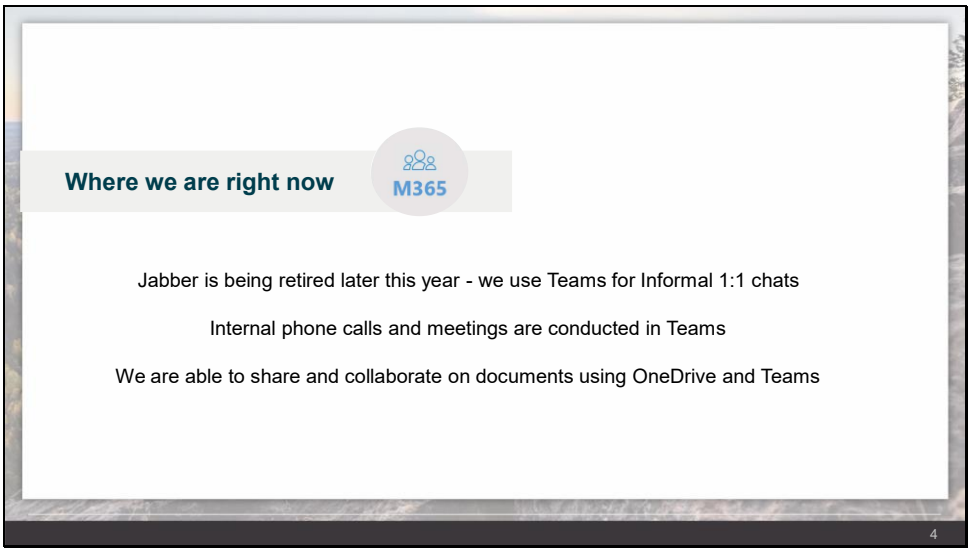
Why are we here? Microsoft offers new tools and new ways to access and use our information. Has this changed the rules for how we manage our information? No!

This session will cover the rules and the tools.



Our learning objectives are quite simple:

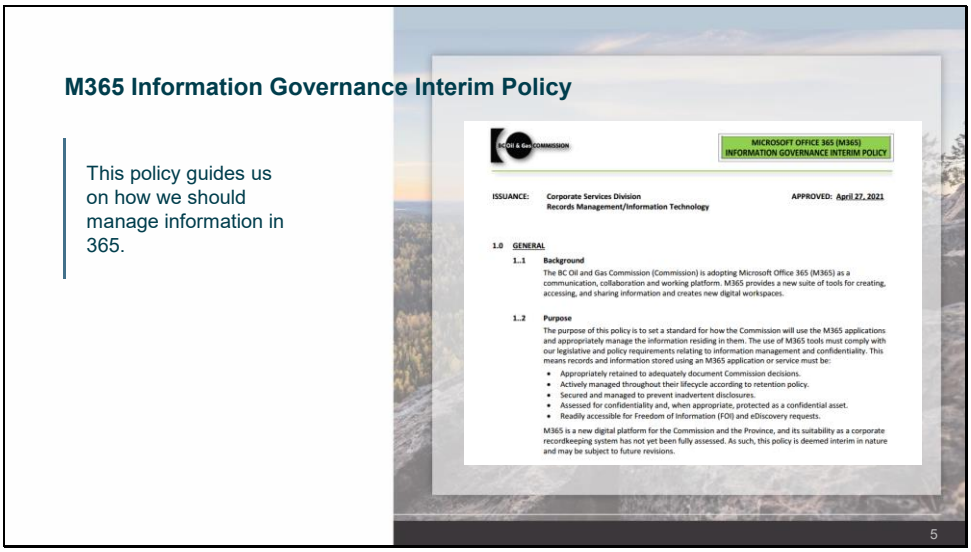
We want you to understand how we will use these new 365 workspaces, our responsibilities for managing information in them, what we mean when we say transitory records, because you will hear us talk a lot about this when we talk about 365, and how to find resources in the future.



Office 365 is the new normal in the Commission and government.

Currently at the Commission we are primarily using the Teams application for conducting meetings, chatting, and supporting internal phone calls.

To support this technology, Records and IT developed a policy to provide a framework for how we use these tools.

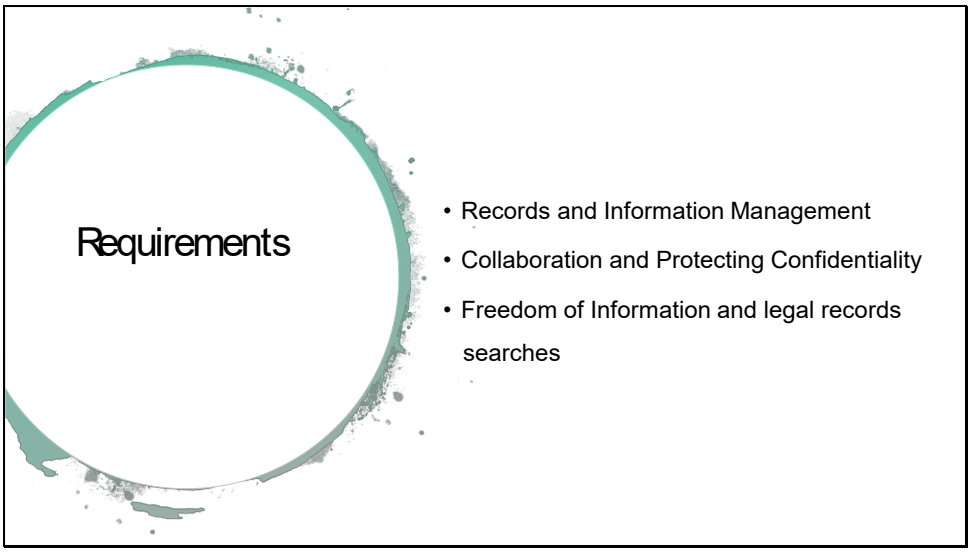


We have called it the M365 Information Governance Interim Policy.

Information Governance is the overall strategy for managing information in an organization. This policy tells us how we should manage information in 365.

It is an Interim policy because we are in a learning curve. This is a new platform for all of us, and we expect that there will be changes as we become more familiar with how we use these tools and what they offer. We are also assessing whether it will be appropriate for managing our electronic records over the long term which will affect the final policy.

We shaped this presentation to the structure of the policy. It's important we all understand our collective and individual responsibilities.



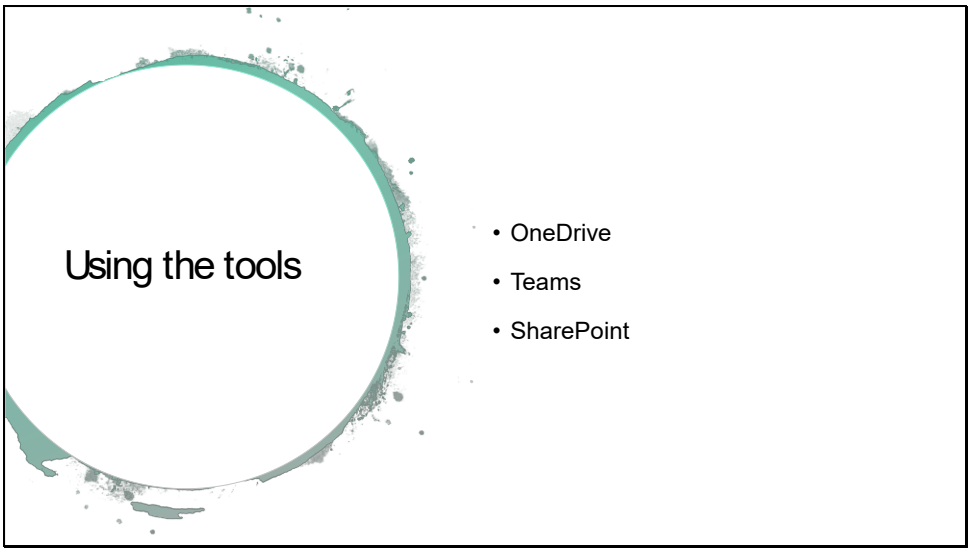
So here are the rules. The first part of the policy covers the requirements which apply to all of us. It is broken out into these elements.

First is records management: official records within 365 workspaces must be saved to an appropriate recordkeeping system, which is usually our shared drives, to ensure Commission decisions are adequately documented and business continuity and operations are supported.

The Collaboration and Protecting Confidentiality section says that users must limit the sharing of sensitive or confidential information, (such as personal information), and outlines what that looks like in 365.

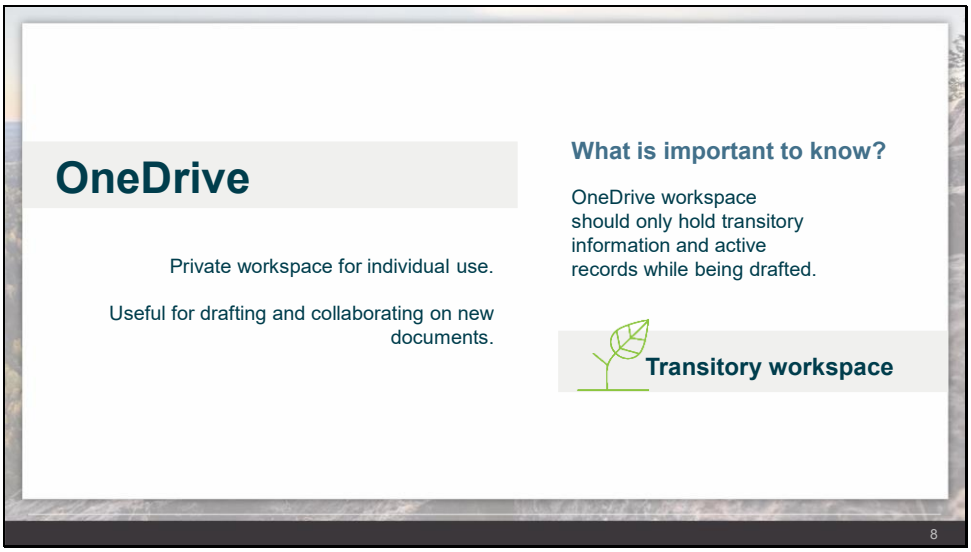
Information in M365, like all Commission information, is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or other legal obligations, and we must be prepared to search for and gather records that are responsive to these types of requests.

To summarize, you have to save your records to the shared drives, protect confidentiality, and remember that all areas of 365 are subject to FOI or legal searches.



The policy then moves to more of what this means to us. It's broken out into application specific sections – meaning OneDrive, Teams, and SharePoint.

First let's talk about OneDrive.



OneDrive is both a platform for sharing documents for collaboration, and to hold transitory information that is useful to you. Like your F: Drive, you are the only person who has access to the records in this space, unless you specifically share something. Because of this, it is not an appropriate place to hold official records for the Commission, such as original records relating to your work.

Let's talk a little more about why we don't use OneDrive for official records:

- You are the only person who sees your OneDrive contents, but your OneDrive content is subject to FOI and legal records searches.
- If you keep official records in OneDrive, they are not accessible by others who may need access to them, and
- We have no way of appropriately managing the records.
- We call these "information silo's" and we want to avoid that.

So, what DO you use OneDrive for?

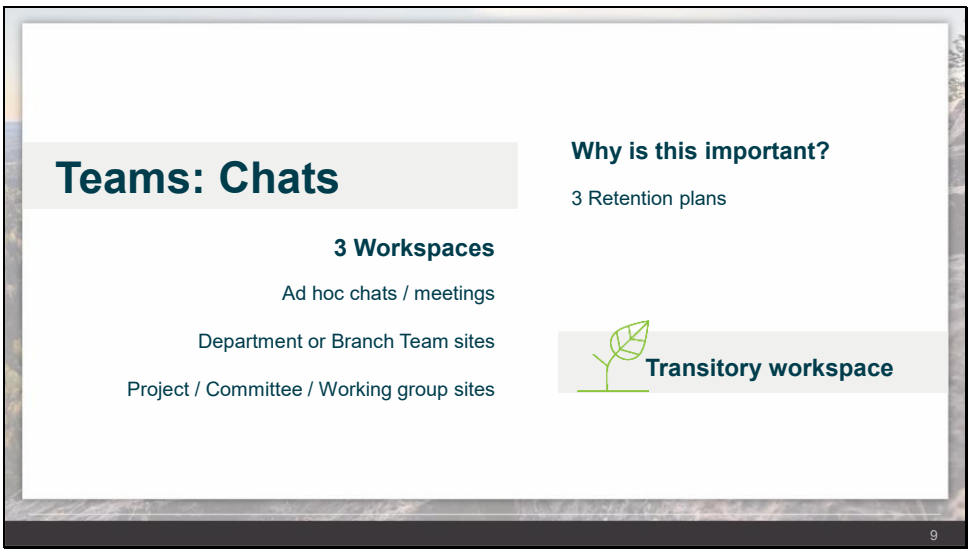
- Working material that you are not ready to share with your team yet
- Sharing a document with select people for collaboration.
- Transitory drafts, and convenience copies
- Personal reference material

You may keep some copies of documents for quick reference, or drafts of documents – but once you have a final version of that draft, or even if it is stalled but might be picked up in a year – it's important to move it out to the shared drive so it becomes part of the record for that activity.

Supervisors may opt to keep a copy of personnel records in their F: Drive or their OneDrive. This may be a copy of their staff's IDP's, or vacation requests. The official records of these are with HR, but we understand the desire to have that information at your fingertips... Since what you have is a copy, kept for convenience, OneDrive is an acceptable use for that. It keeps it secure and accessible to you.

Just remember that Commission records should be filed in our shared drives. When you are finished working on that document in OneDrive, move the final over to your shared drive.

Now let's talk about Teams.



Teams is probably our most used application for M365 so far, and the policy dictates both how we use it and how long we keep the chat data within it. We have all started using Teams for meetings and chats.

You may have also noticed that IT is rolling out Teams sites. There are two types of Teams sites – Teams built specifically for each branch or department, and Teams for specific working groups, committees, or projects. The intended use for each site determines how long we keep the information in it.

It is important to understand that Teams is not an appropriate recordkeeping system. Teams is for transitory communication. This is key. We don't want to hold official records within this workspace.

With that as our basic principle, we manage Teams chat data in three ways:

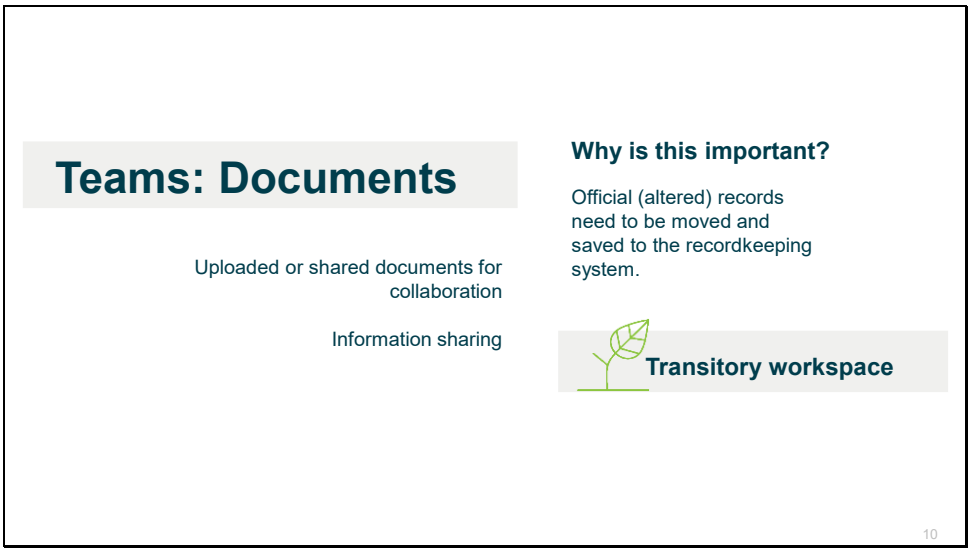
- One-on-one chat messages are automatically deleted after 10 days, and this is fine, because we are only using this for transitory purposes.

- Department/branch chats (within a Teams Site) are automatically deleted after three months. This includes both private channels and branch channel chats.

- Project/committee/working group conversations (within Teams Sites) are kept for the duration of the project, then deleted at the end of the project, after the lead has confirmed that any official records within the site have been pulled or copied out.

This is important for you to know because it gives you timelines for capturing official information out of Teams.

Most of you will have attended a Documenting Commission Decisions workshop, and those principles apply here. Any official or critical information in Teams must be captured in the recordkeeping system, this includes context for a business decision, or a record of a decision. This means that if your chat conversation has strayed into decision making territory, you will want to summarize or copy it out before the 10 days has lapsed.

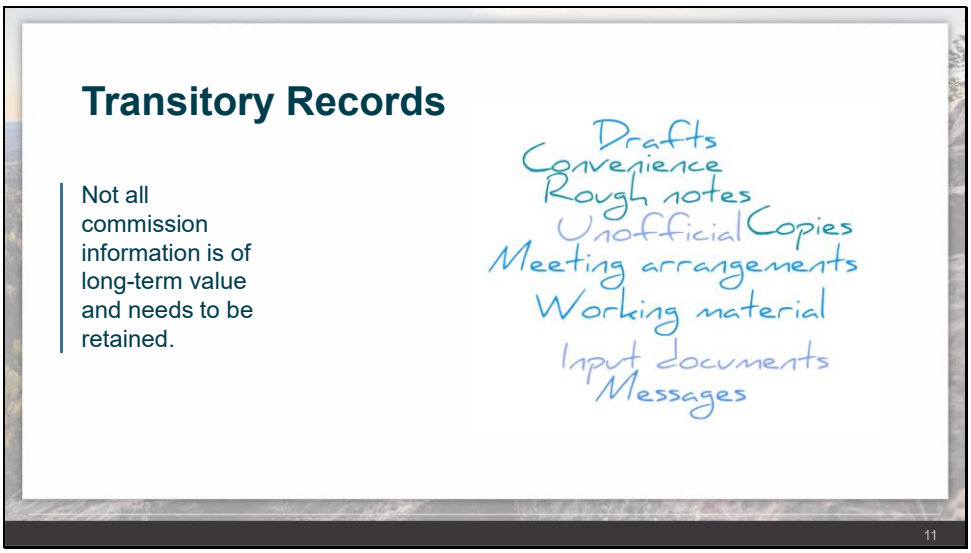


The chat retentions we just talked about do not apply to documents in Teams. This means that documents are not auto-deleted the way chats are – uploaded documents reside in a team site until the Teams site is closed. It also means that we have to manage them more actively.

As you may have figured out, there are a few ways to share documents in Teams, and that is a whole other conversation. Our focus is on what you do with the documents once you are finished with them. As we have said, Teams is transitory workspace, so if you have created or completed a document in this space, it's important to remember to move it out to the recordkeeping system.

For example, if you use Teams for collaboration on a document, make sure one of you takes that final version of the document, and puts it into the appropriate folder on the K: Drive. If it is sitting outside of a Teams site, in a 1:1 chat, you won't see that document after 10 days, so make sure you stay on top of this.

Let's talk about Transitory Records since we have referred to them so many times.



The phrase we keep using – TRANSITORY RECORDS. Per legislation, all recorded information is a "record", and needs to be managed according to retention schedules. This means that our Teams chats, our Word documents, all the things we are creating and receiving are records, but there are different categories of records. All records need to be managed according to approved information schedules (i.e., ARCS/ORCS/Transitory Schedule).

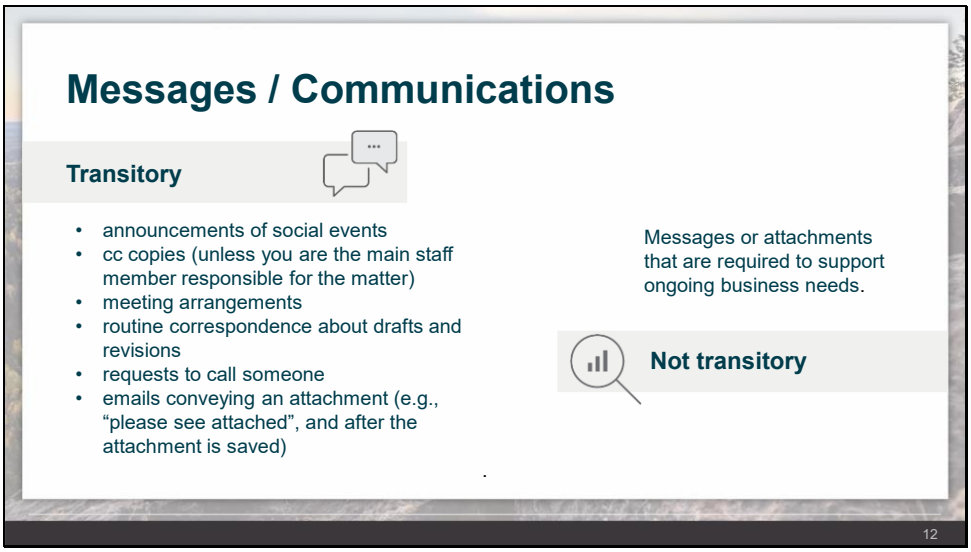
Transitory information is information of temporary and/or low value that is only needed for a limited period of time in order to complete a routine action or prepare a subsequent record (such as a new version). Each of you has the authority to delete transitory records when your use is complete.

So, these may be rough notes and working materials. **Context** and **content** help determine whether a record is transitory. For example, preliminary notes relating to planning a training session are more likely to be transitory than notes relating to drafting regulations or establishing a new commission program.

Other transitory records:

- Copies kept for convenience and quick access
- Printed out agendas for meetings (not that we are doing that these days!)

It's fairly common sense, but let's break it down a bit more.



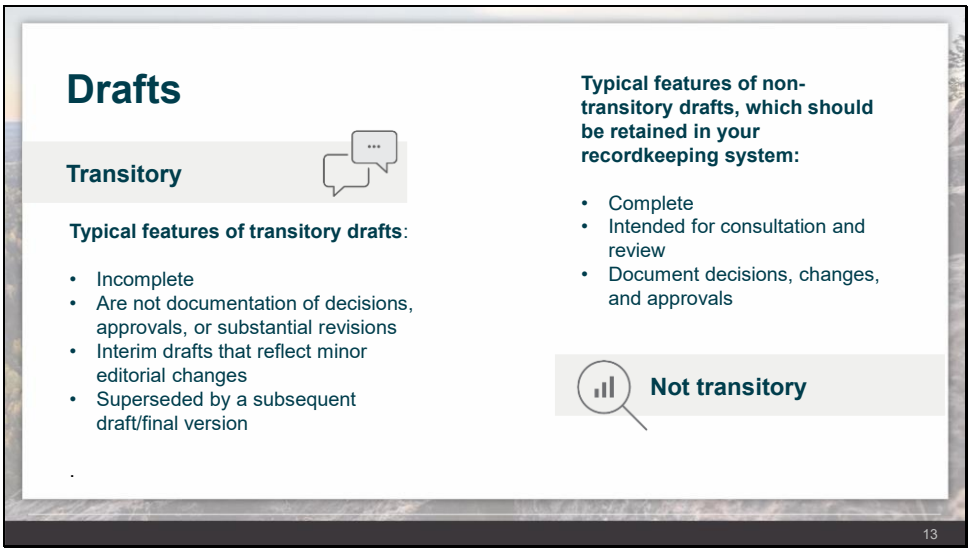
Messages can take many forms - email, instant messages such as Teams chats, social media postings, or voice/video message recordings. Transitory messages are messages of only passing value that do not support or document a business activity or decision. We have examples of transitory messages on the screen, which covers:

- Emails which announce social events, such as our Tuesday Trivia Challenges, or cc copies (unless you are the main commission member responsible for the matter, because then you hold the official record)
- Meeting arrangements
- Routine correspondence about drafts and revisions
- Requests to call someone, and
- Emails conveying an attachment, once the attached record is saved

Messages that are required to support our business needs are **not transitory** information. Due to their content, or the context they provide, they must be retained (such as an email documenting a policy decision or advice, chat agreeing to a course of action, or social media post that is the initial announcement of a new program).

Just a housekeeping note: once these “not transitory records” have been saved into the right folder on the K: Drive any copies of the messages may be considered transitory and deleted. For example, once you have copied an email to a folder on the shared drive (your recordkeeping system), you can delete the original in Outlook. It is a good practice, because if you leave it in Outlook, it may cause confusion down the road to whether you have filed it or not.

Let’s talk about transitory drafts.



Transitory drafts are incomplete versions of a document which have been superseded by a new version. They will typically contain minor edits. Once a subsequent draft or finished record has been developed and filed, transitory drafts are no longer needed.

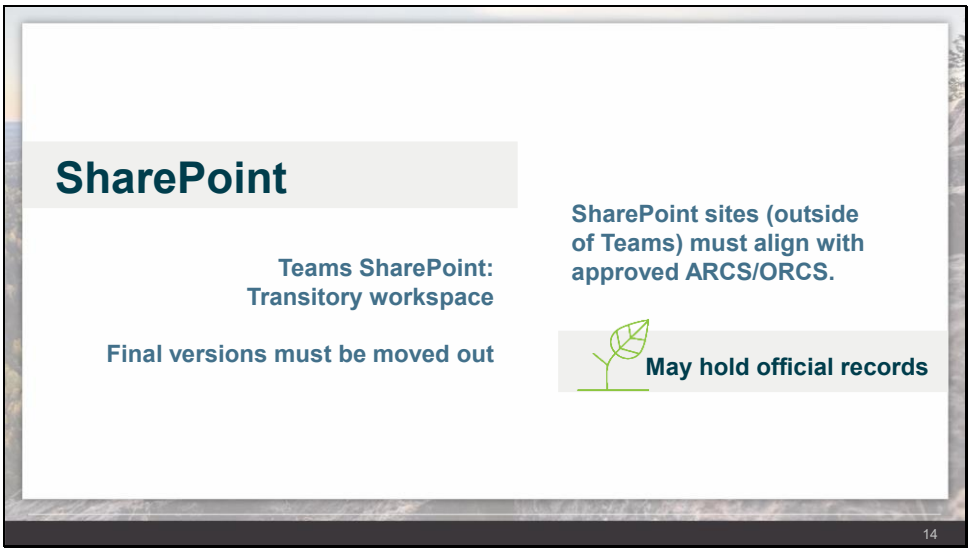
On the other hand, a draft which document decisions, has substantial changes, or approvals is not transitory. Consultation versions with input from stakeholders are not transitory. These should be retained. Draft legislation, audit reports, and other significant drafts are **not** transitory.

And of course, we must never destroy any transitory information that may be relevant to a current/anticipated *FOIPPA* request or legal discovery.

This concludes the transitory records part of the training.

We want to make sure everyone understands this because it helps clarify what we mean when we say a workspace, such as OneDrive, or Teams should only hold transitory information in the longer term. And if you do have official information, it should be moved to the recordkeeping system on the shared drive. This ensures that the records are preserved, managed, and easily found for future use.

Back to the last 365 tool we are going to talk about – SharePoint!

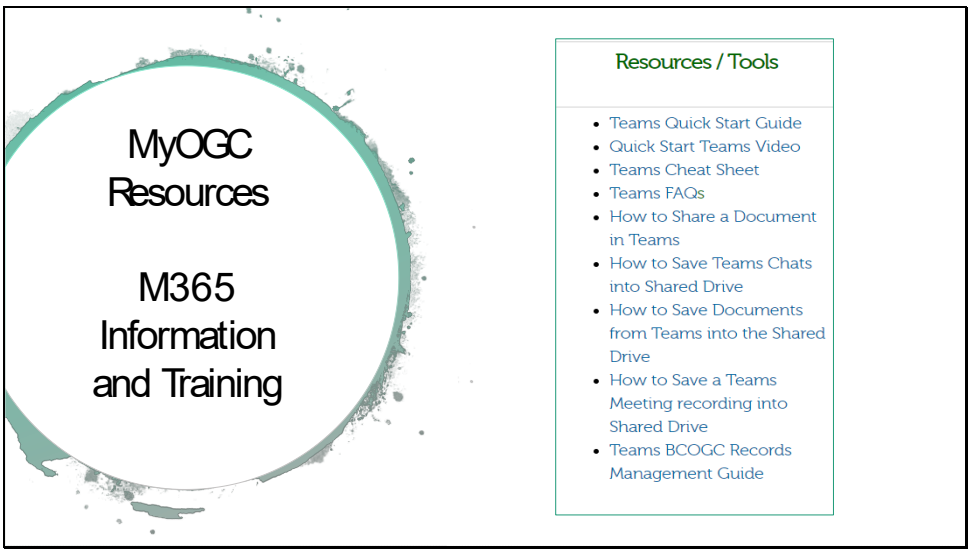


The policy also addresses SharePoint. There are two main uses of SharePoint in 365, SharePoint inside of Teams and SharePoint outside of Teams. As you get your Teams sites for your branches and projects, you will notice that it uses SharePoint as the platform for sharing and collaborating on documents. Each Teams SharePoint is specific only to that Team and intended for short-term use and collaborative purposes, not for storing records.

SharePoint in Teams is a transitory workspace. Official records created within this workspace must be moved out of the Teams environment and saved to the recordkeeping system on your shared drives.

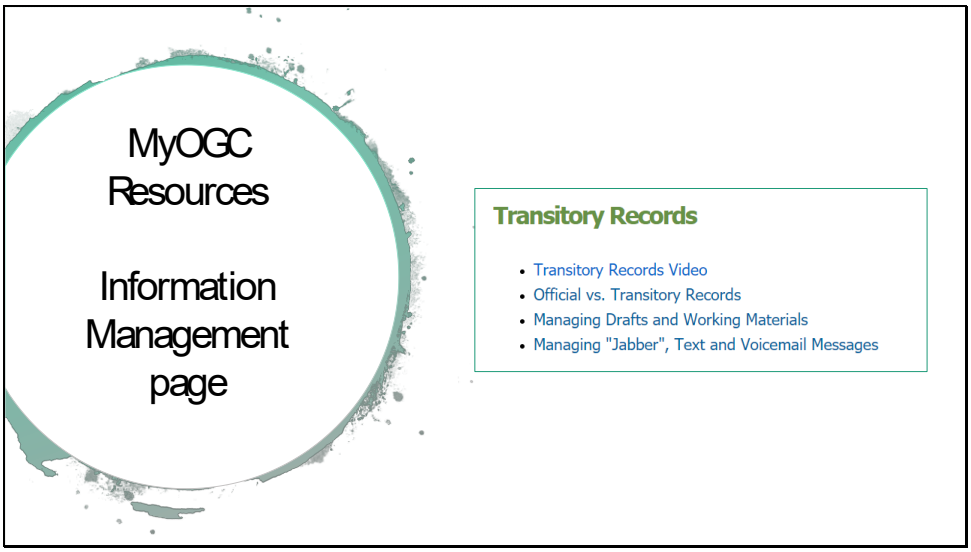
SharePoint sites outside of Teams are typically used as broader communication tools or collaboration hubs at a corporate level. These SharePoint sites are retained for a longer duration, and content must be managed according to records lifecycles and retention rules. Site structure must align with approved information schedule classifications. Our branch will be working with you, and IT, when these sites are developed to ensure we put the right foundations in place.

You have learned a lot today… so let's end this by showing you where you can find resources for future reference.



There are a wide range of M365 guidelines that have been created by your IT and records teams. They are on the M365 information and training page, under the Technology tab of MyOGC. For example, in the Teams section, which we show here, you will see How-To guides related to saving Teams chats into the shared drive, saving documents, general records management guides, etc.

Check them out if you have questions.



As a final slide, we want to point out additional guidance related to transitory records. You will find these under the Corporate Tab, on the Information Management page. We encourage you to use these resources.

Thank you for your time! As a reminder, our branch is always available to help you and answer questions.

BC Oil & Gas COMMISSION

Shared Drive Organization

in the BCER

CHAOS
TO ORDER

3 Goals

3 Goals

1. De-duplicate
2. Shorten long file paths

3. All folders clearly relate to an ARCS/ORCS classification

Information Schedules:

ARCS = Administrative Records Classification System
Covers: committees,
human resources,
financial management,
agreements
IT projects,
etc…

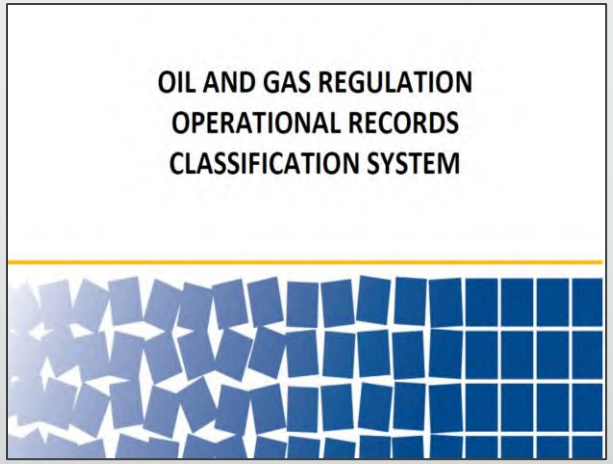
ORCS = Operational Records Classification System
Covers operational BCER work which supports our mandate

Information Schedules:

ARCS = Administrative Records Classification System

ORCS = Operational Records Classification System

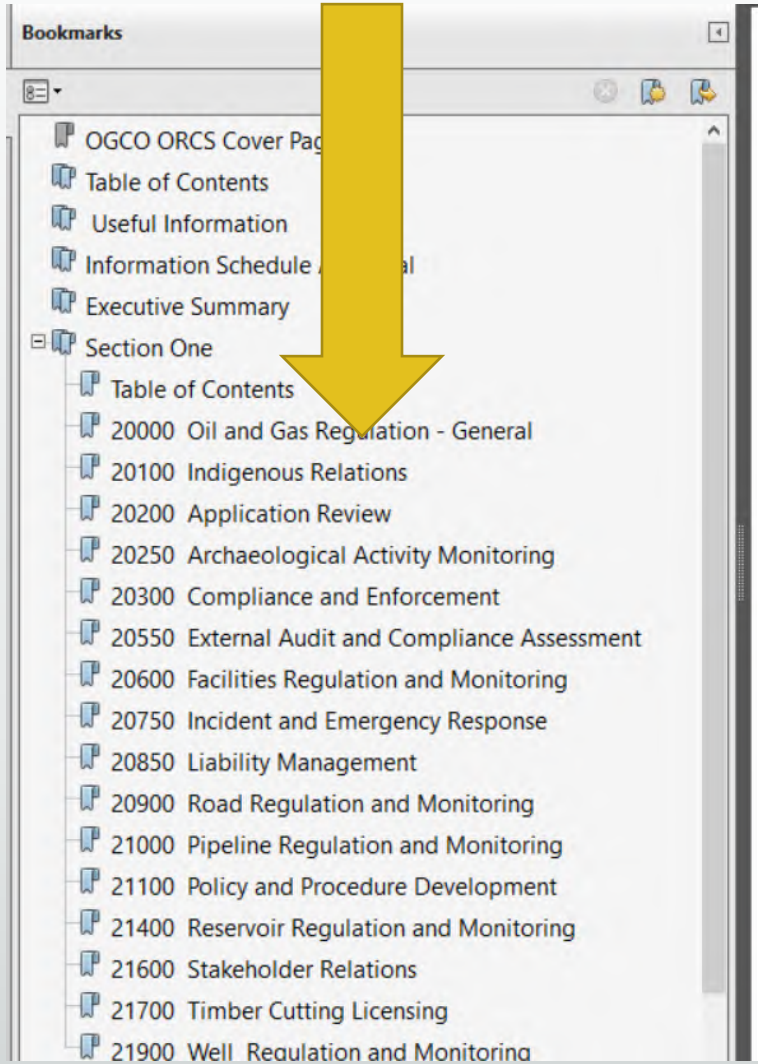
Just to be clear… ORCS = this

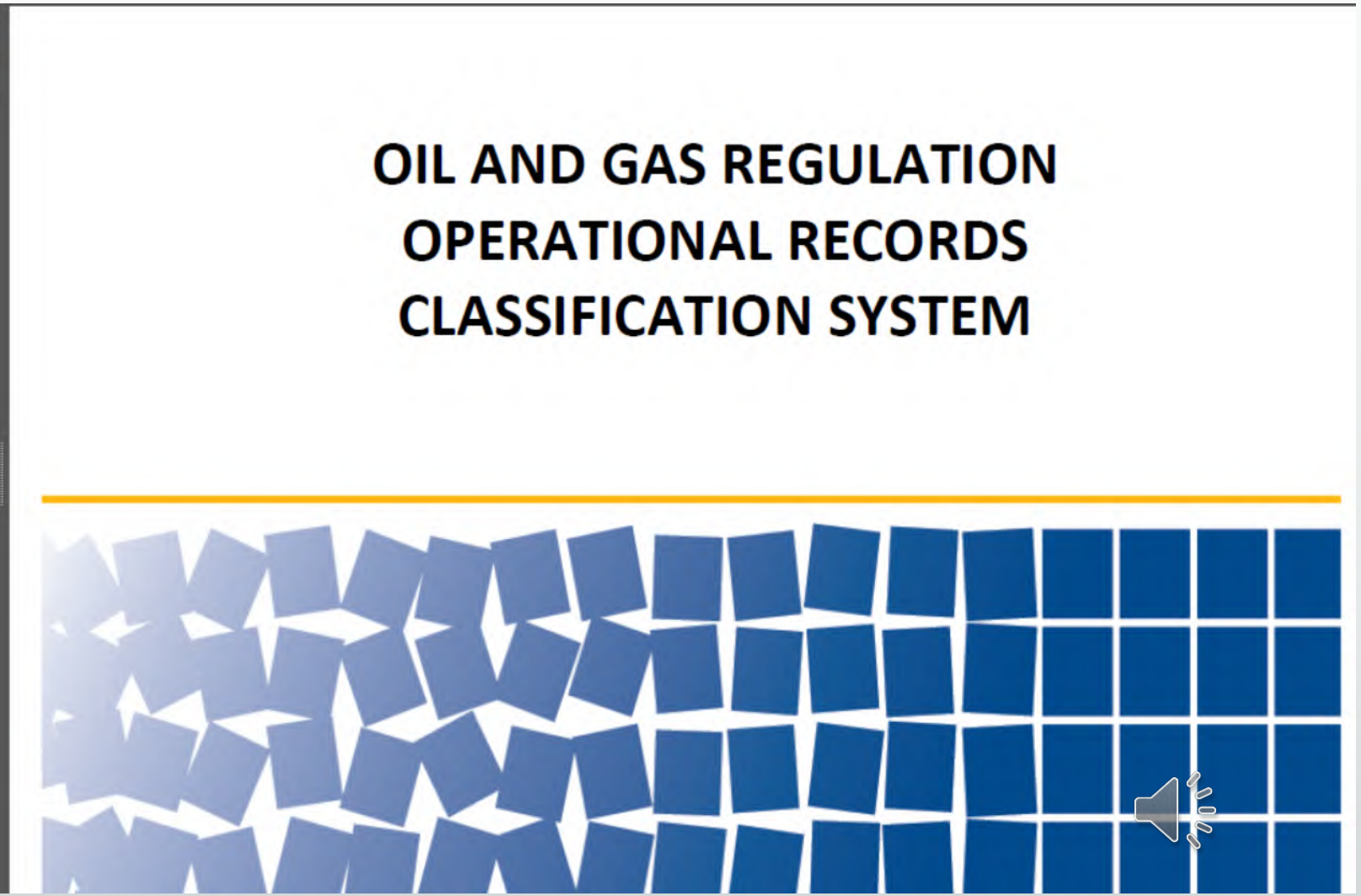


Not this:

OGCO ORCS
Primaries

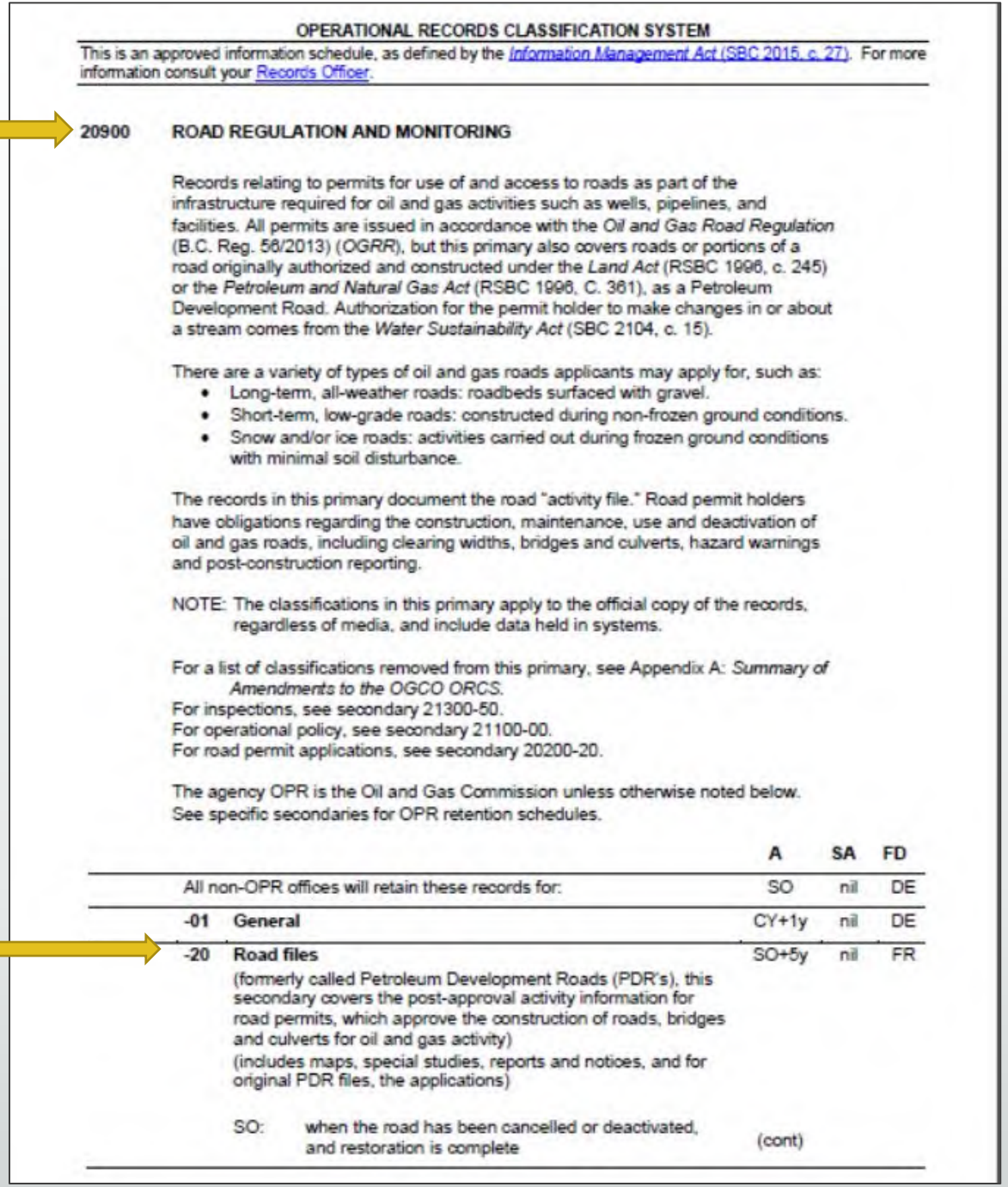
See how they relate to what we do?





ORCS Primary 20900

ORCS Secondary -20



OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Officer.

20900 ROAD REGULATION AND MONITORING

Records relating to permits for use of and access to roads as part of the infrastructure required for oil and gas activities such as wells, pipelines, and facilities. All permits are issued in accordance with the *Oil and Gas Road Regulation* (B.C. Reg. 58/2013) (*OGRR*), but this primary also covers roads or portions of a road originally authorized and constructed under the *Land Act* (RSBC 1996, c. 245) or the *Petroleum and Natural Gas Act* (RSBC 1996, C. 361), as a Petroleum Development Road. Authorization for the permit holder to make changes in or about a stream comes from the *Water Sustainability Act* (SBC 2104, c. 15).

There are a variety of types of oil and gas roads applicants may apply for, such as:

- Long-term, all-weather roads: roadbeds surfaced with gravel.
- Short-term, low-grade roads: constructed during non-frozen ground conditions.
- Snow and/or ice roads: activities carried out during frozen ground conditions with minimal soil disturbance.

The records in this primary document the road "activity file." Road permit holders have obligations regarding the construction, maintenance, use and deactivation of oil and gas roads, including clearing widths, bridges and culverts, hazard warnings and post-construction reporting.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS.*
For inspections, see secondary 21300-50.
For operational policy, see secondary 21100-00.
For road permit applications, see secondary 20200-20.

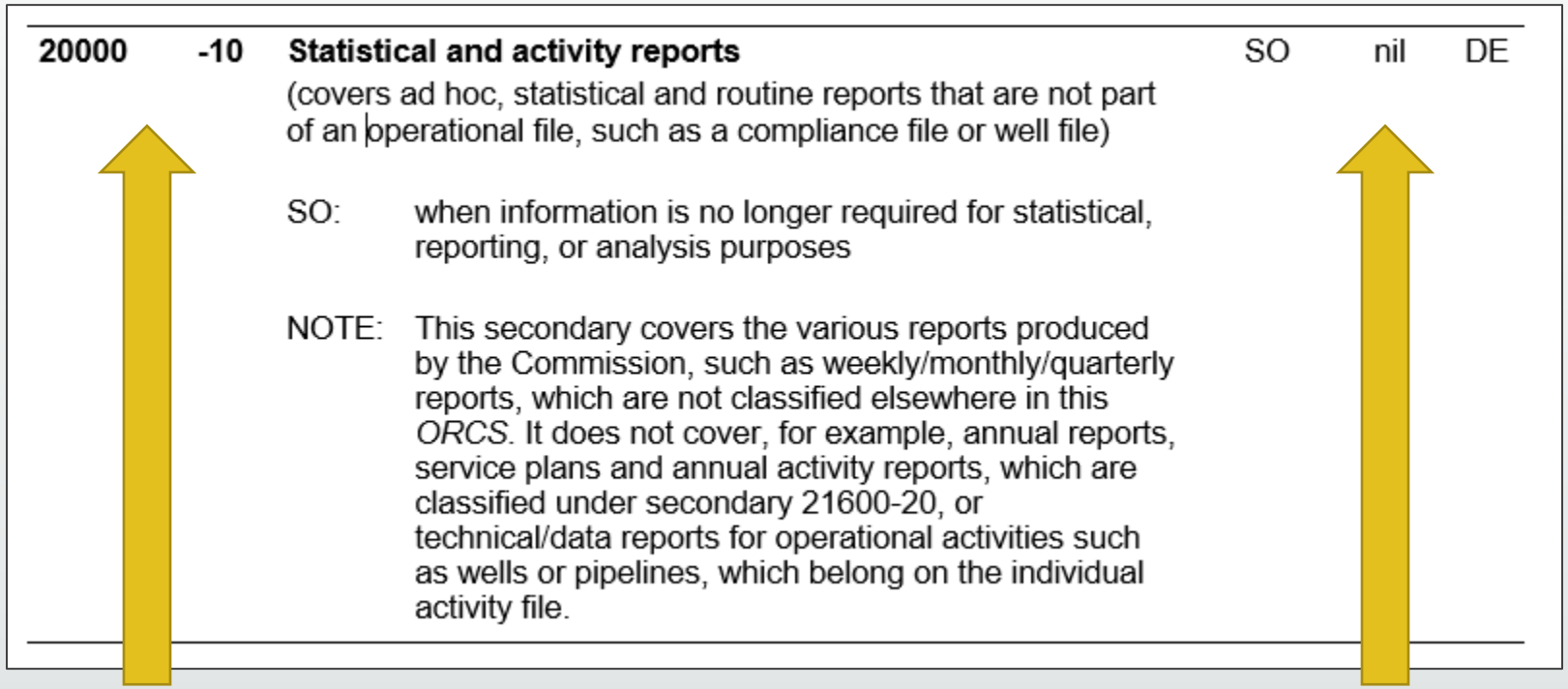
The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
All non-OPR offices will retain these records for:		SO	nil	DE
-01	**General**	CY+1y	nil	DE
-20	**Road files** (formerly called Petroleum Development Roads (PDR's), this secondary covers the post-approval activity information for road permits, which approve the construction of roads, bridges and culverts for oil and gas activity) (includes maps, special studies, reports and notices, and for original PDR files, the applications)	SO+5y	nil	FR
	SO: when the road has been cancelled or deactivated, and restoration is complete	(cont)		

The classification number is 20900 -20.

It covers activity records for roads.

ORCS Secondary



20000	**-10**	**Statistical and activity reports** (covers ad hoc, statistical and routine reports that are not part of an operational file, such as a compliance file or well file) SO: when information is no longer required for statistical, reporting, or analysis purposes NOTE: This secondary covers the various reports produced by the Commission, such as weekly/monthly/quarterly reports, which are not classified elsewhere in this *ORCS*. It does not cover, for example, annual reports, service plans and annual activity reports, which are classified under secondary 21600-20, or technical/data reports for operational activities such as wells or pipelines, which belong on the individual activity file.	SO	nil	DE

Classification number
20000-10

Retention codes
which provide the
management plan for these records

An ARCS primary

102 - Administration, Staff Meetings

ARCS > Administration

Records relating to ministry/agency staff meetings, including internal management-level meetings.

Record types include correspondence, agendas, minutes, and reports.

non-OPR NOTE: Offices will retain non-OPR copies of records for SO nil DE

Primary-Secondary	Records Series	OPR		
		A	*SA*	*FD*
102-00	Policy and procedures	SO	nil	DE
102-01	General	CY+2y	nil	DE
102-20	Staff meetings DE= Staff meeting records can be destroyed upon authorization of the Records Officer because information concerning significant agenda items are included in ministry/agency executive committee meetings, which are selectively retained by the government archives under the Executive Records schedule (102906)	CY+2y	nil	DE

Previous | Next

Herding Cats
1
2
3
4
5
6
7
It CAN be done

To-Do List for Shared Drive Projects

- ✓ *Reduce duplication*
- ✓ *Reduce long file paths*
- ✓ *Assess security requirements*
- ✓ *Create good structure*
- ✓ *Move files to new folders as necessary*
- ✓ *Train staff for maintaining structure*

What it looks like:

- Audit and review files 975-40
- Lists spreadsheets and registers 100-05
- ORCS Development 432-40
- RM projects and plans 432-60
- Travel files 1240-20

- _Forms & Templates
- Contract Mgmt 1070-20
- Financial Reconciliations 920-20
- MOUs and Agreements 146-45
- Presentations 324-40
- Procurement 1070-30
- Staff Meetings 102-20

Thanks for watching!

Shared Drive Projects script. *(★ means change slide)*

Hi! Thank you for taking the time to learn about why we want to organize Shared Drives in the Commission, and what our shared drive projects goals are. ★

Shared Drives are our current record keeping system in the Commission. However, they are not structured for being record keeping systems. Introducing structure to commission drives allows us to *manage* our electronic records rather than store them, and lays the path for our future goal of an EDRMS. ★

We have 3 goals for shared drive projects: ★

1. Remove unnecessary duplication – makes the records easier to manage because the focus will be on the official records, and reduces storage costs ★
2. Shorten long file paths – we have a 250 character limit to file paths, which includes document titles. If we go longer than that, we are at risk of our records not being backed up properly. Naming conventions can help with this. Our aim is to keep it intuitive, but not long. ★
3. Every single folder relates directly to an ARCS / ORCS number.

We have a few "rules" when it comes to managing Commission records. One key rule is that every record that is not transitory must have an ARCS or ORCS classification that applies to it, so you can know how long to keep it and what to do with it when that time is done - delete it, (following our destruction processes), or transfer it to the government archives. ★

This rule is born in legislation, which says that you can only destroy a government record in accordance with an information schedule.

ARCS covers administrative records – the housekeeping and common records that you will find in any government organization. ★

ORCS are the custom-built schedules, covering the records that are unique to your organization from the rest of government. ★

They are structured the same way; they just apply to different types of records. They both provide classification numbers for arranging your records, and retention periods, which tell you what the lifecycle is for managing your records.

Next we are going to go through a quick primer to ARCS and ORCS. We are just going to touch on what you will need to understand decisions we make during this project. ★

A building block to ARCS and ORCS are primaries. Primaries are based on a function – what you are doing. This may be negotiating agreements (in ARCS), or doing compliance work (in ORCS).

Primaries have a primary number, which is the first part of your classification number, and a title, which describes the function.

Within each primary are secondary categories, each one for records that supports the primary function. A secondary has a two-digit number assigned to it, and that is the second part of your file number.

A secondary also has a retention period, which lays out management plan for the records. The retention period is broken into a three-stage lifecycle, and uses simple codes, to be system friendly.

There is a guide at the beginning of our ORCS, to help interpret the codes. We call the guide "useful information"

As we said, ARCS and ORCS are structured the same way – they just look slightly different from each other. This is an ARCS primary.
These are the documents we talk about when we say we are "mapping" your folders to ARCS/ORCS, and these are the classification numbers you will see in your newly structured shared drive.

So what does a shared drive project look like?

RIS does analysis on your folders, creating a duplicate report and a long file path report. We work with you to start cleaning those areas up.

Then we start to create the structure. We talk with you to find out what security permissions need to be applied. We may talk about naming conventions if that makes sense for your team. Our goal is for the structure to work for you.

When we set up the structure, and assign the classification numbers to the folders on your shared drive it will look something like this.

As we work in your project, we can explain details, but we hope this high level description makes it clear what our aim is, and why are we doing this. We look forward to working with you!

Organizing Shared Drives in the Commission

A guide for the DIY folks

Records and Information Services
2020

Table of Contents

Background: why we are doing this 2

3 Goals for a Shared Drive project 3

Commission Shared Drive principles 3

Getting started 4

- Key elements to a successful shared drive project 4
- Steps to organizing a shared drive 4

What does this look like? 6

BACKGROUND: WHY WE ARE DOING THIS

We are building a strong and compliant Information Management (IM) program in the Commission. One of our key goals is to help you effectively manage your electronic records. This goal requires the right tools, processes, technology and support. There are three main steps to get us where we need to be:

UPDATE OUR ORCS

Making sure our Operational Records Classification System (ORCS) reflects the Commission's current business environment - the work we do now, and the records we maintain to support that work.

IMPLEMENT THE ORCS

Run a series of Shared Drive organization projects so we are managing our records with ARCS and ORCS.

This implements the ORCS, and is essentially a (really big) clean up project!

INTRODUCE EDRMS

Once the shared drive projects are complete, and our records organized, we will be ready to onboard an Electronic Document Management System (EDRMS).

This is where we want to be.

Organizing our shared drives is a critical part of the IM goal. As you may have noticed, the information on our shared drives is arranged in a variety of ways right now. “Organizing,” means we arrange our electronic records according to our new ORCS and to ARCS. This process allows us to:

1) Have our files organized in a consistent manner.
2) Know the requirements for managing our records, rather than just storing them forever.

Doing this will:

- increase findability of Commission information;
- support collaboration;
- assist with business continuity through staff change; and
- help us to be better stewards of the information we hold.

Applying ORCS and ARCS structure to shared drive records provides a functional logic, and consistency.

THE 3 GOALS FOR A SHARED DRIVE PROJECT

We have three basic goals for our shared drive projects:

1. **Reduce unnecessary duplication**
   Doing this helps us to focus on managing the official records, reduce storage costs, and have more efficient file searches.
2. **Reduce long file paths**.
   We have a 250-character limit for file paths, which includes document names. Any file paths longer that that are at risk of not being backed up.
3. **Ensure that every folder clearly relates to an ARCS or ORCS classification.**

And of course, create a useable environment where people can keep and find their records.

COMMISSION SHARED DRIVE PRINCIPLES

- Top-level folders will clearly match an ARCS or ORCS classification. All content within the folder belongs under that classification, unless otherwise indicated.
- We will use the classification title, or a close match, and follow that with the classification number. Exceptions to using the classification title will be to provide a more intuitive environment for staff.
- Folders with series of files in them will have a “Closed” folder at the top, and staff will move the closed projects, investigations, or other files into that closed folder on an ongoing basis, to assist with easy file management.
- If the retention for the folder is based on a calendar or fiscal year, folders will be established accordingly (i.e. a folder each for 2016, 2017, 2018 and so on) to make file management easier
- Staff will use naming conventions to help control versions, and identify final copies of documents.

GETTING STARTED

KEY ELEMENTS TO A SUCCESSFUL SHARED DRIVE PROJECT

- **Training.** Provide basic training so all affected staff understand why we are doing the project, and what we mean when we talk about retention, transitory records and ARCS/ORCS.

- **Have clear roles and processes.** Ensure everyone knows what they will be doing in the project, and what the go-forward plan is.

- **Plan it out**. Think through the details such as security permissions for the folders, what the structure needs to look like, what classifications apply, and contact your Records and Information team for advice.

- **Communicate, communicate, and communicate**. Moving people's records has to be done with care, so you don't negatively impact business or cause undue stress. Plan out the best way to communicate when files will be moved, how to help folks find the new file locations, and how to involve them in understanding the new system.

Before you get started, see the ARCS/ORCS User Guide for understanding records language, and watch our 4-minute video on Organizing Commission Shared Drives

Here is an overview of the process, and snapshots of our approach.

HIGH LEVEL STEPS FOR ORGANIZING SHARED DRIVE FOLDERS

1. Evaluate your current structure.

2. Work with RIS to find duplicates, long file paths, and identify ARCS / ORCS classifications.

3. Plan the new structure. Set up a folder and start building the new folders within it (see the next section for how this might look).
   Considerations:

   a. If you have existing folders that can be classified by an ARCS or ORCS category, you may just need to rename that folder with the file number on it.

b. If you have folders with fiscal or calendar year retentions, set up a year structure inside that overall folder (example: a travel folder, with sub-folders for each fiscal year). See next section for examples, and refer to naming conventions for dated folders.

c. For folders that have "project" type of material, and an SO retention, put a _Closed folder in there, so when the project is closed, it can easily be dragged and dropped into the _Closed folder, and staff will only see active projects when they first open that space into the folder. This will keep the folder cleaner.

d. Create a high level folder called _Final Disposition. When you find folders that are closed, and at the end of their lifecycle, put them in the _Final Disposition folder, so we can process them. This is an important clean up element!

   TIP: we usually mirror your new structure in this folder, so closed files can be managed easily in the future.

e. Are there folders that require unique security permissions? Permissions are assigned at the root folder level, so when you are planning your structure this may affect where you put specific folders.

f. Often at this point the structure is in its "first phase". Once you start going through folders you may identify new categories of records, so expect it to grow as you move through the project

4. Establish naming conventions. Are there specific ones for your team, beyond the standard Commission naming conventions?

5. Meet with your team and go over the new structure. Have the ARCS/ORCS classifications you have used on hand, so you can speak to the retention plan if people ask.

   a. Establish a plan to meet with team members to talk with them about "their" records, confirm classifications, and what goes where in the new structure.

   b. Be sure to discuss the nature of the records with staff, rather than making assumptions. This is key to assigning the correct classifications, which ensures the records are findable, and will have the appropriate retention applied.

6. Once everyone is comfortable with the new structure move it out to the root level. You may want to move (copy/paste) the old folder structure into a folder called something like "previous folders", so your team sees the new structure first - and you don't have to sort out old from new.

7. When moving files, make sure you:

   a. Find a time when staff won't be working with the documents.

b. Inform staff ahead of time so they know the information is moving, and tell them where the information is moving to.

c. Move the files at the scheduled time.

d. When the contents of an old folder have been moved out, assign an “x” at the front of the old folder to indicate that it’s empty. Put a shortcut in the empty folder to the new location, to help people who go to the old folders out of habit.

8. Carry on moving folders / documents into the new structure!

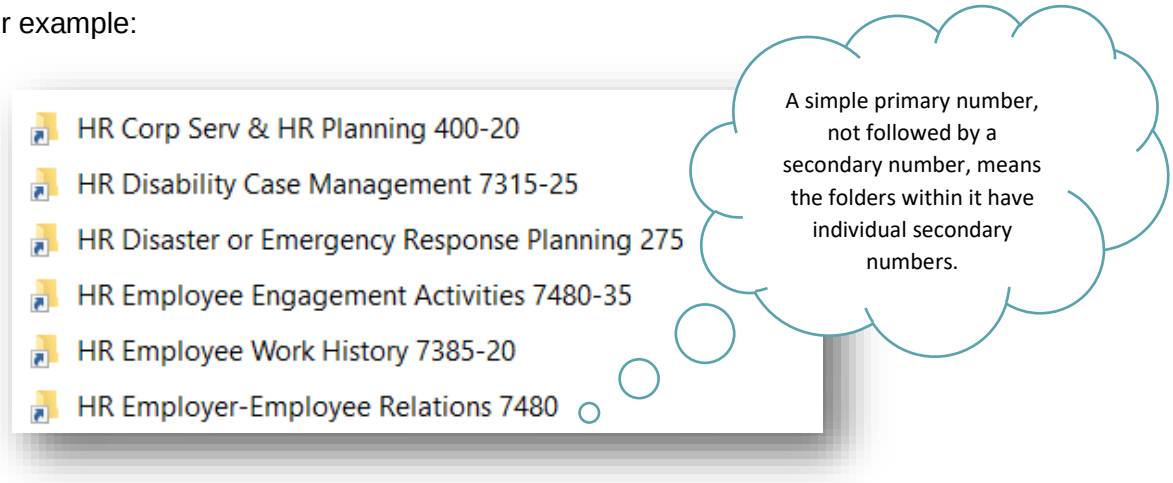
See the next page for examples of what this looks like.

WHAT DOES THIS LOOK LIKE?

Here is an example of a shared drive using ARCS numbers on folders. Note that they are arranged alphabetically, by classification title, with the ARCS numbers following the title:

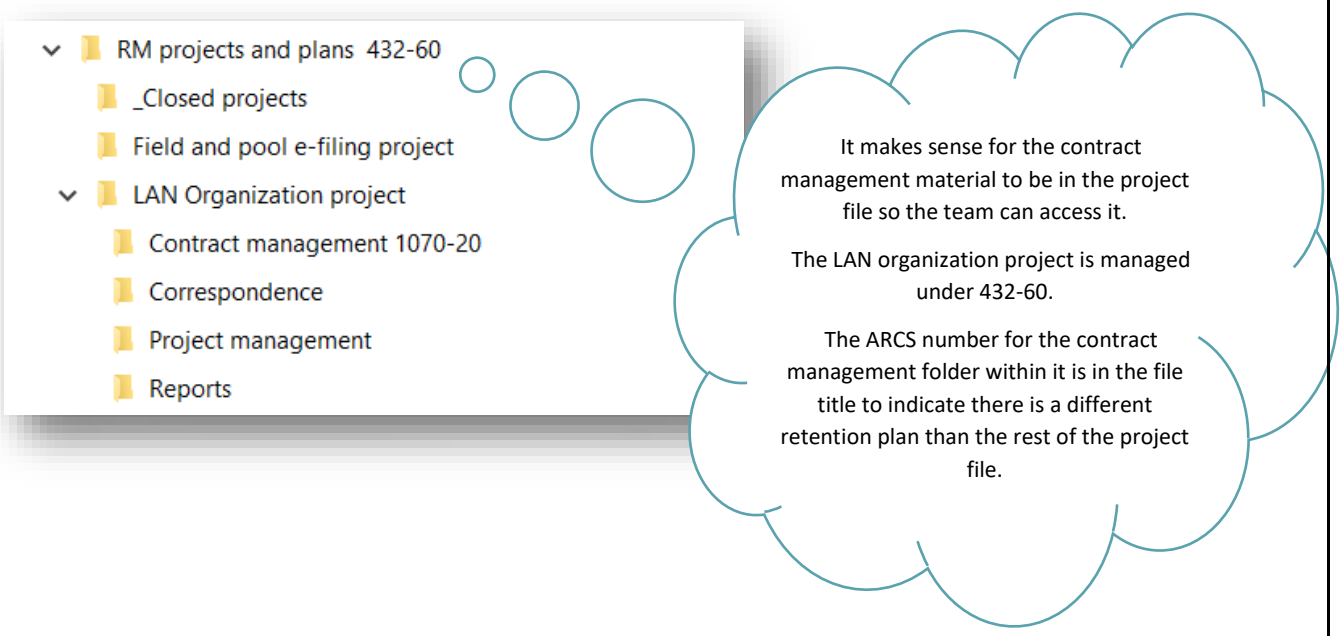
The sub-folders within these can be free form. The expanded version looks like this:

Here is another example:



Per the example above, sometimes you will want to group related files together, even though they have different secondary classifications. In this case, the highest-level folder will have a primary, and inside that folder are secondary classifications:

Alternatively, you may nest one folder into a file which has a different classification altogether, because it makes sense operationally… this makes managing the folders a bit more complicated, but convenience and practicality may make it worthwhile. See the image on the next page:



You will see that while we are introducing structure and have some guiding principles, we are also trying to provide some flexibility so people can intuitively find their files.

Records and Information Services are happy to assist in the project planning process! We can help in the following ways:

- ✓ Provide de-duplication reports and long file path reports to assist in cleaning up your current drives.
- ✓ Help you find correct classifications for your information, which will form the basis of your new structure.
- ✓ Advise on best practices for naming conventions, if you think those would help your team.
- ✓ Provide templates for folder management tips, or cheat sheets, and
- ✓ Cheer with you for your progress!

Please contact Records and Information Services if you are ready to start a shared drive project, or if you have questions about our records program initiatives.

And check out our resources on our MyOGC Information Management page.

Shared Drive Organization Projects
Selection criteria

We weight the selection for shared drive organization projects accordingly:

Criteria	Description
Branch Readiness	Branch Readiness looks like this: • Branch can provide a primary contact for the project • Staff have time to attend training and planning sessions, and • Staff can meet with RIS on an as-needed basis.
ORCS Implementation	A priority for RIS is to implement the ORCS. This supports: • momentum from the ORCS modernization project, • continuity for staff who have already been thinking about records, and • provides value for time spent on ORCS development.
Location	We want to share our work to all corners of the Commission, and may prioritize a project if it is in a location that we have not directly supported recently.
Business Cycle	It is critical to project success to align with natural ebbs in business cycles; we want to be careful not to start a project during “crunch times”.
Complexity of project	If we have a small gap of time, we may prioritize smaller projects that we know we can complete in the time available.

Shared Drive Organization

Engineering project

Presenter:

Mahia Frost, OGC Information Management Specialist

Special Guest:

Marion Villines, Shared Drive Organizer Extraordinaire

Shared Drive Organization

Project drivers – PGA and IMA requirements

Overview of your shared drive

Going forward

(a) correspondence,

(b) investigations,

(c) surveys,

(d) reports,

(e) data,

(f) background information,

(g) assessments,

(h) designs,

(i) specifications,

(j) field reviews,

(k) testing information,

(l) models,

(m) simulations,

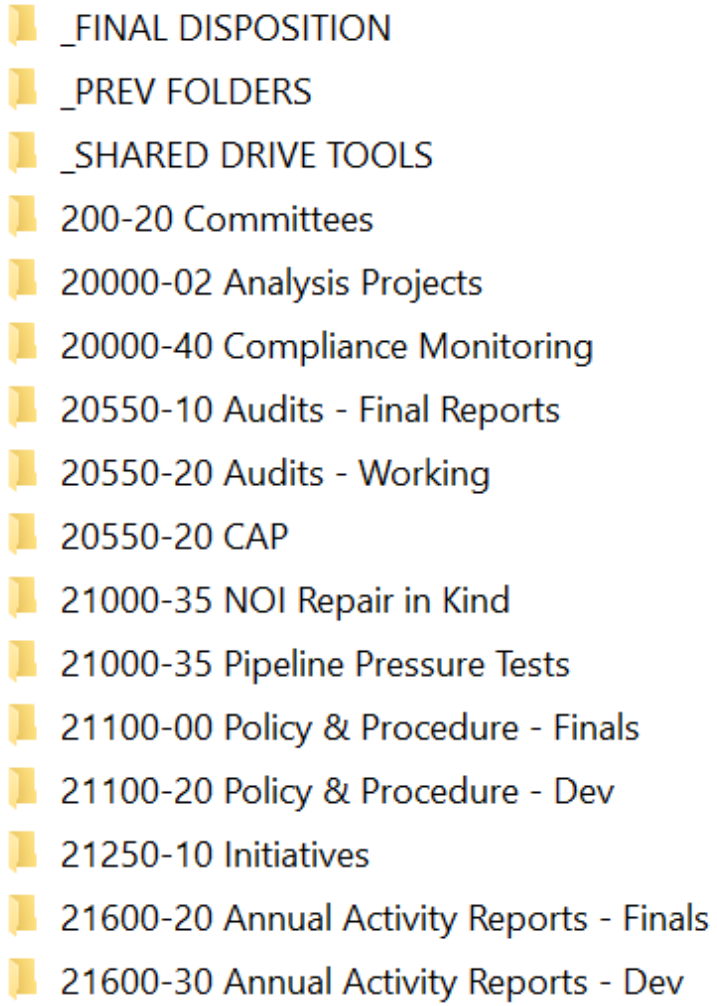
Bylaws of Engineers and Geoscientists BC

CHAOS
TO ORDER

Shared Drive Overview

Project goals:

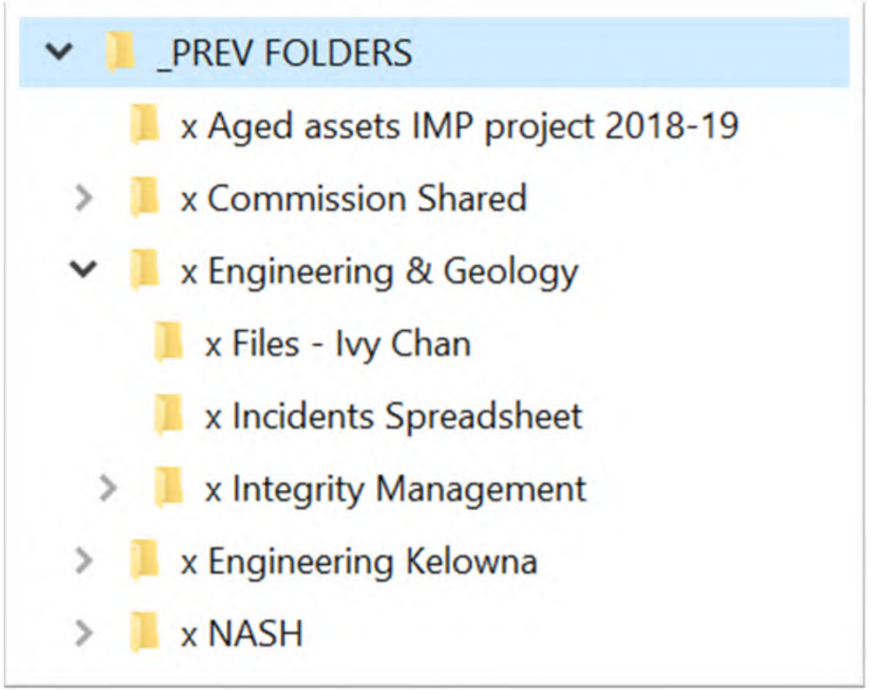
- All folders have an ARCS/ORCS classification at the top
- All documents within a folders belong to that classification/topic



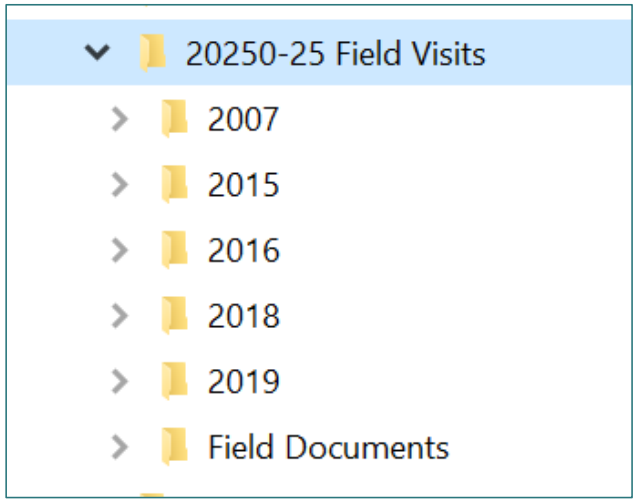
Standard Folders

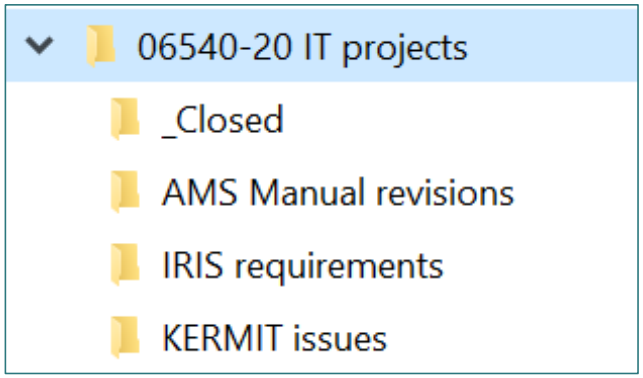
_FINAL DISPOSITION

_PREV FOLDERS



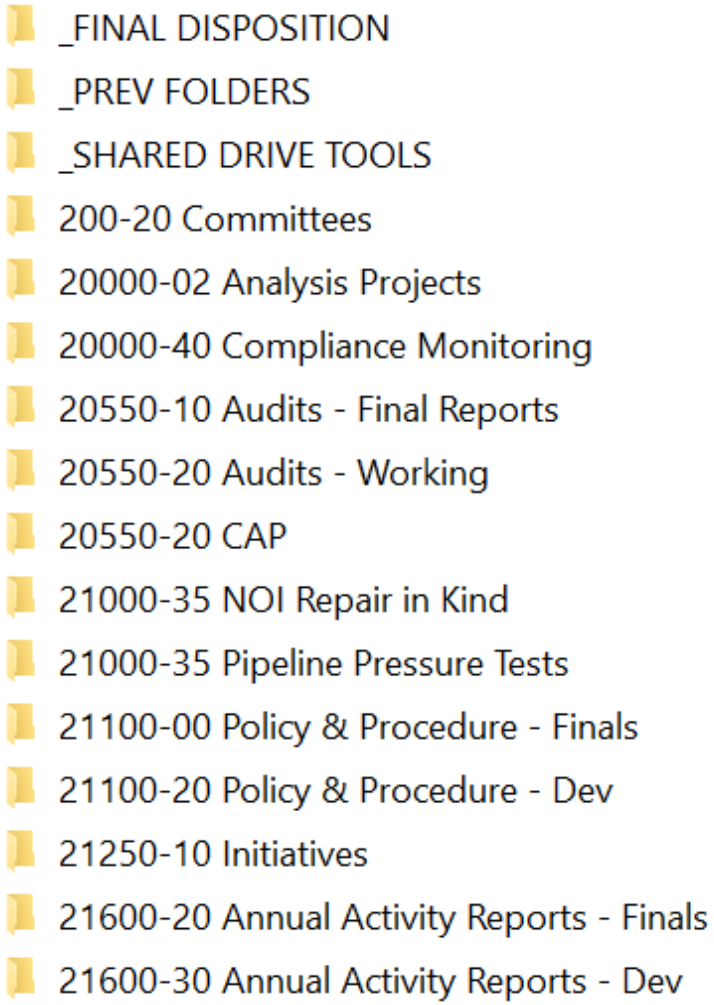
Some of the ways we organize documents in the folders.





Using the system

Focus on what you are doing to find the right home for your information.



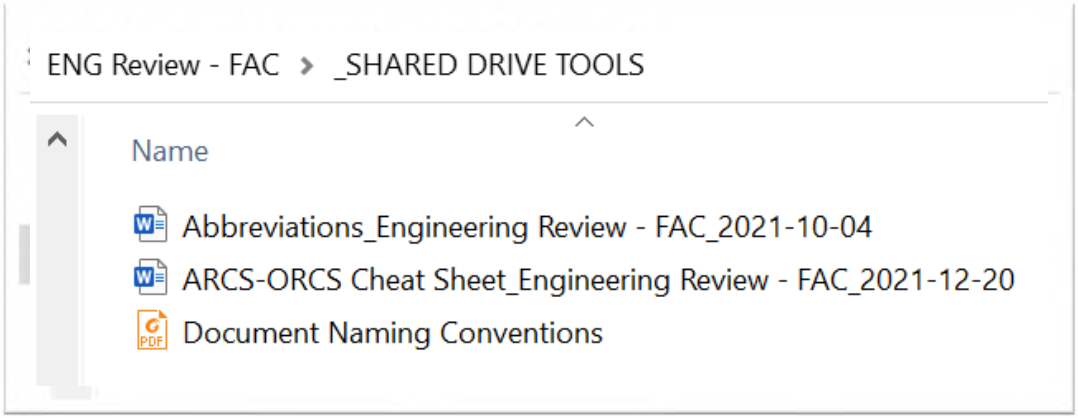
Best Practices

Keep contents clean – delete transitory material.

File relevant emails into folders so you have a whole record.

Standard Folders – Shared Drive Tools

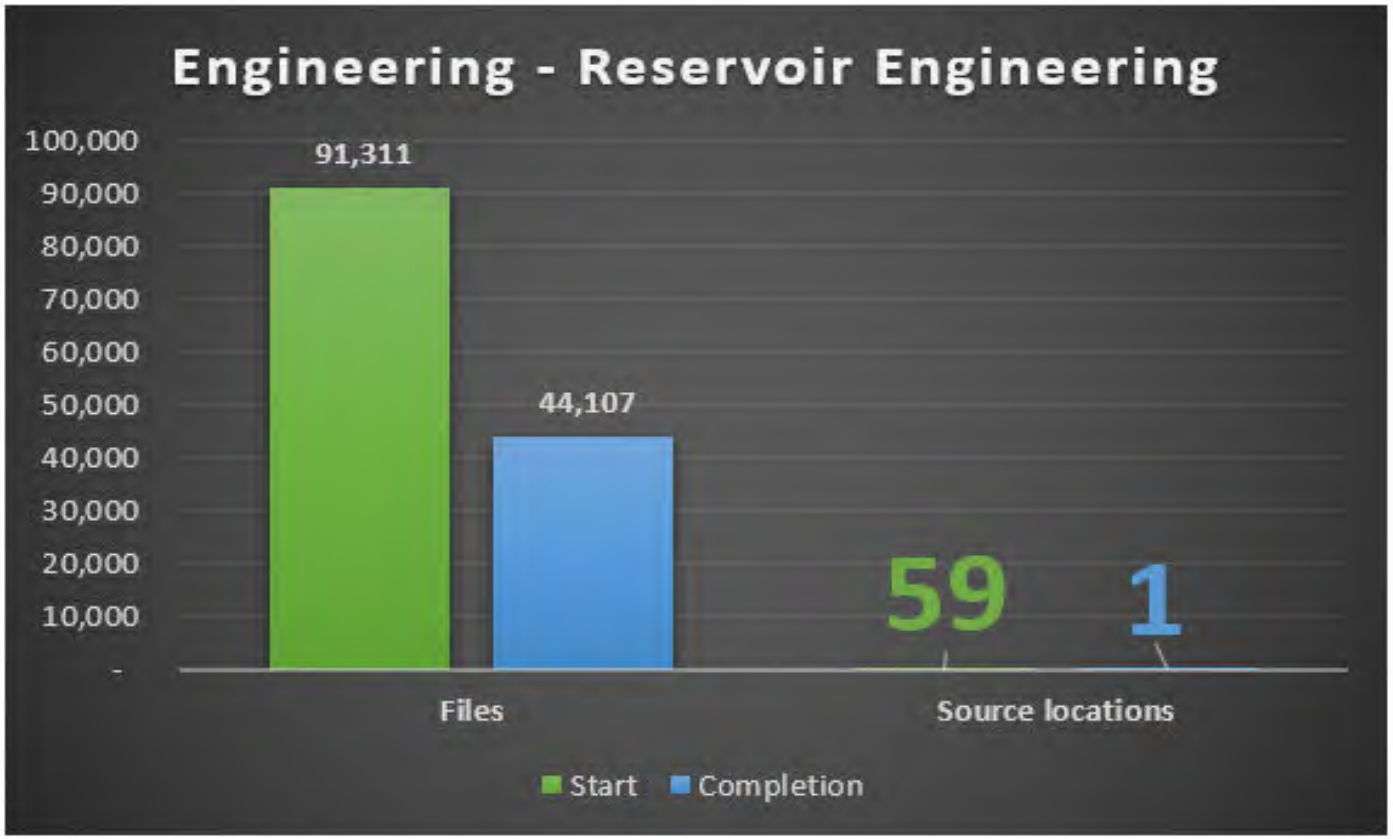
_SHARED DRIVE TOOLS



What to do next.

Herding Cats
1
2
3
4
5
6
7
It CAN be done

YOU JUST HAD A BIG "HOUSECLEANING"!



Review of records dating back to 1996 - 26 years of electronic information!
Eliminated duplicate and obsolete records: **52% reduction** in files/documents.
Harmonized records from 59 sources to (basically) one place.
Project duration: 5 months, including pre-project analysis time.
Fantastic involvement and support from the Reservoir Engineering team!

YOU JUST HA
"HOUSECLEA

Engineering - Reservoir Engineering

1

rce locations

tronic information!

on in files/documents.

Harmonized records from 59 sources to (basically) one place.

Project duration: 5 months, including pre-project analysis time.

Fantastic involvement and support from the Reservoir Engineering team!

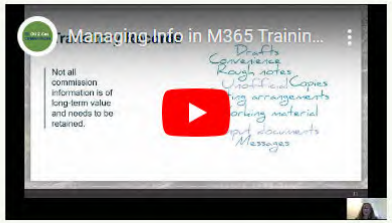
RM Resources

Information Management in M365

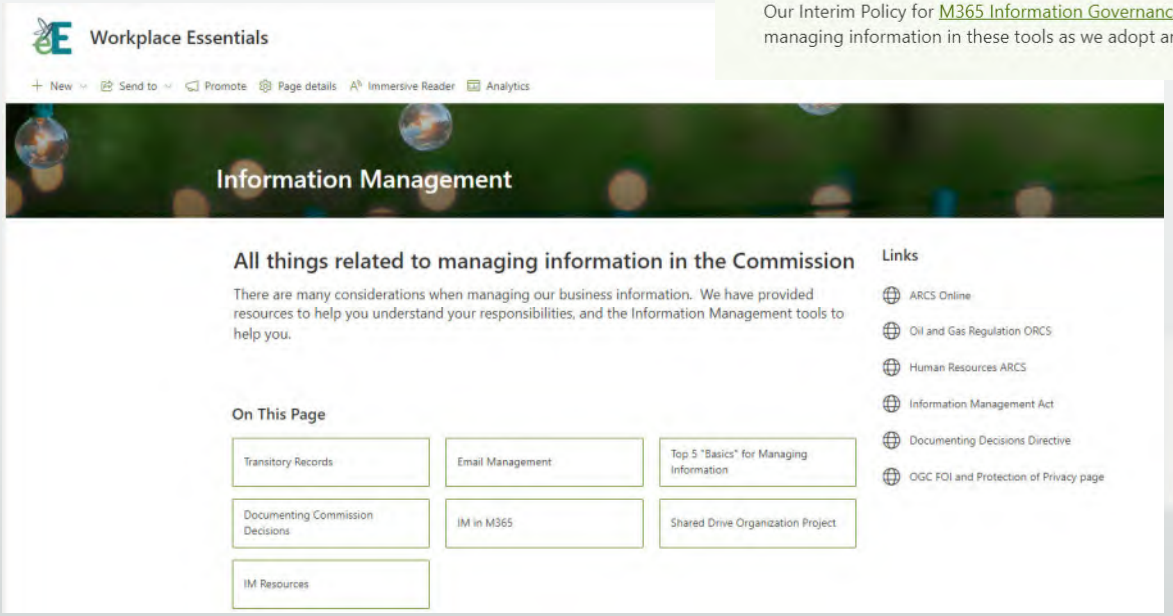
Microsoft 365 offers new tools for creating and using our information, but the Information Management rules haven't changed. Here is some guidance on how we manage our information in the M365 environment.

- Managing Information in Teams
- Managing Information in OneDrive
- Managing Information in SharePoint
- Teams - Sharing Documents in Teams
- Teams - Saving Documents from Teams to Shared Drives
- Teams - Saving Meeting Recording to Shared Drives
- Teams - Documenting Chats

Our Interim Policy for M365 Information Governance outlines the Commission's approach to managing information in these tools as we adopt and adapt to this platform.

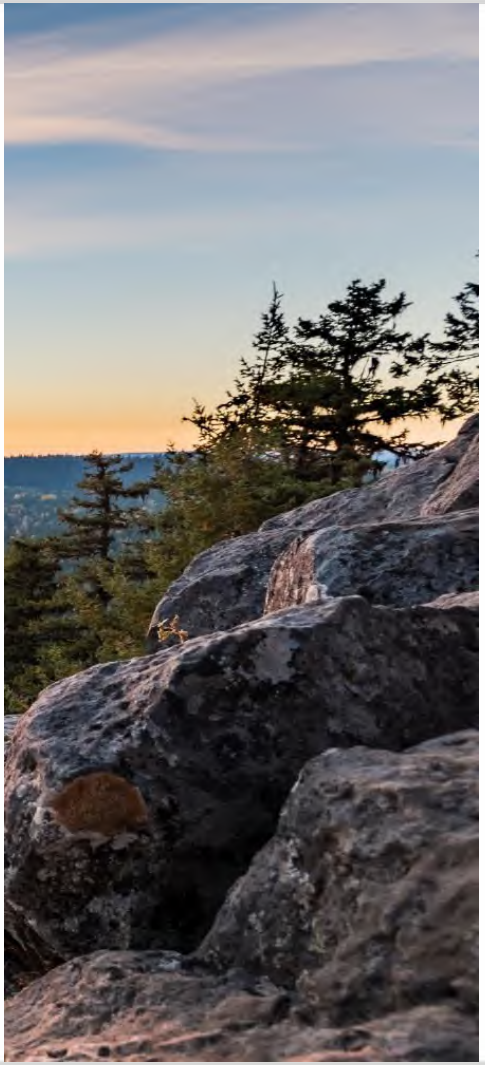


Managing Information in M365



Please reach out with any questions

Thanks for working with us!



Copy and paste this ‘3’ onto any slide you wish. It will automatically populate to the correct slide number.

BC Oil & Gas COMMISSION

Managing Email Guide

June 2021

Table of Contents

Overview 3

Using your Commission email 4

Using personal email accounts 4

Tips for sending email 6

Tips for managing email discussion threads 7

Managing your email

- Commission emails are Commission records 8
- Deciding what to keep or delete 8
- Organizing email in Outlook 10
  - Working with Folders 10
  - Working with Categories 11
  - Working with Rules 12
- Saving email records outside of Outlook 12
  - Saving email – Responsibilities 13
  - Tips for saving email records 13
  - Preferred email preservation formats 14
  - Saving email records on your Shared Drives 15
- Deleting email appropriately 15
  - Working with the Clean-up tool 16
  - Working with Auto-Delete folders 17
  - Working with Assign Policy tool 17
  - Emptying Deleted items on exit 18
  - Exercise: Find and delete emails from distribution lists 18

Contacts 20

Appendix A: Managing Phishing and Spam Quarantine 21

Overview

Email is a fundamental communication tool for Commission employees. The volume and diversity of the emails we create and receive on a daily basis can make managing them seem like an impossible task. This guide will help you navigate the world of email so it can be as effective a tool as possible.

Good information management practices can help you manage your emails. Implementing simple routines will help you to wade through your emails and separate the valuable messages from the rest. Proper email management will not only make your life easier, it will ensure that important commission information is available to meet business and legislative requirements.

This guide will help you to comply with the *Freedom of Information and Protection of Privacy Act (FOIPPA)*, the *Information Management Act (IMA)*, our Information Management Policy, and Use of IT Resources Policy, including how to:

- understand security responsibilities surrounding email
- understand your responsibilities when using your email account
- determine what emails need to be kept and keep those emails in ways that protect their authenticity and integrity
- determine what emails you can delete
- delete those emails appropriately using simple tools available in MS Office 2016 for Windows

.

Much of the material in this guide originates from the BC Government Records Service. The Commission version is a collaboration between Information Systems & Technology, and Records & Information Services.

Using your commission email

When do I have to use my commission-issued email account?

As an employee, you are required to use your commission email when conducting commission business (except in extenuating circumstances).

Not all of our business requires the use of email — but when it does, you are required to use a commission account. This includes when you are working outside the office.

Can I use my personal email account or an email account related to another organization for personal use while at work?

Per the Use of IT Resources Policy, reasonable personal use of commission-issued IT device by employees is permitted as long as you follow these rules:

- Your use of non-commission email account on a commission- issued device should be limited during work hours and must not interfere with your duties and responsibilities.
- Any use of personal email for personal use while at work must be lawful, must not compromise the security of commission IT resources or commission information, and must not be used for personal financial gain.
- The use of a commission-issued computer, laptop, smartphone or other device must be consistent with the Employee Oath of Conduct and Ethics, whether that use is directly related to your employment duties or not.

Using personal email accounts

Can I ever use my personal email account for work purposes?

Only in rare, extenuating circumstances are you permitted to use a non-commission email account for commission business. It must be absolutely necessary to do so.

For example, you may not forward work emails or documents to your non-commission email account simply to work on them at home or to create a convenience copy.

In the rare circumstances where you are unable to securely access your commission email account, you must always follow these steps:

- Send or receive the least amount of confidential information necessary to deal with the extenuating circumstance until you are able to use commission email again.

- Send a copy of the email to your commission email account. A good practice at this step is to note the circumstances that prevented you from accessing your commission email account.
- Delete the email from the inbox, sent items and trash of your non-commission email account as soon as possible. You should also send an email note to your commission email account noting that you have deleted the commission record(s) from your personal email account and have not made any copies of the information.
- Resume use of commission email as soon as possible, including using commission email for the remainder of an interaction that began via personal email.

You must exercise additional caution if the email contains personal information. Most email account providers – such as Gmail or Hotmail – store your emails outside of Canada and the *Freedom of Information and Protection of Privacy Act* prohibits personal information held by the government from being accessed or stored outside of Canada, except in limited circumstances.

A word on protecting sensitive information…

You are responsible for ensuring that any confidential information you are working with is protected. Email is not a secure communication channel. Given the ease with which email messages can be distributed and accessed by others, you need to take extra precautions when working with confidential information.

Limit the amount of confidential information transmitted over email. Use your best judgment or, if you are uncertain, check with your supervisor. Avoid using email to send confidential, sensitive, protected or secret information, except where there is a specific business requirement to do so.

See our Managing Confidential Information Guide for more information, or call Records and Information Services if you have a question.

.

Tips for Sending Email

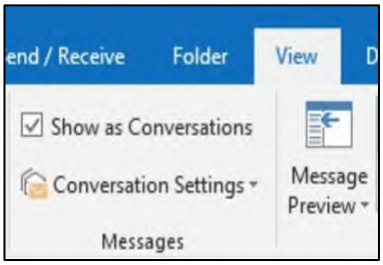
- ✓ Keep email to a single topic. If the topic changes, create a new email thread. If the email covers two or more topics, consider filing it in two places.
- ✓ Be specific in the subject line. Create a clear, concise, and descriptive title. Use the subject line to indicate actions, purpose and due dates.
- ✓ Use your signature block for all outgoing email messages going to recipients outside your working group. If your email contains important decisions or actions, always include your signature block.
- ✓ Limit the number of recipients. Only include recipients who are expected to take action or make a decision on a topic. Use the 'cc' option when sending messages to recipients for informational purposes.
- ✓ Limit the use of attachments. Whenever possible, post your document to a shared location (e.g. on shared drives) and send a link in the email (see Appendix A at the end of this guide for how to insert a hyperlink into an email)

Descriptive subject lines are important for managing email and are helpful aids for determining whether you need to save an email or if you can delete it. Some recommended subject lines are:

Action by <date>
Follow up:
Question:
Answer:
Request:
As requested:
As promised:
FYI
Thank you!

Tips for Managing Email Discussion Threads

- ✓ Do not forward unnecessary information from previous emails to new recipients. Before you include another person on the thread, delete any information that is not needed for completing the task at hand. Avoid unnecessary duplication.
- ✓ Recommended practice: the person who initiates the email thread be responsible for ensuring the thread gets filed. Recipients may also save emails, depending on the content and context of the message.
- ✓ Use the conversation clean-up tool with caution. When a conversation has split into separate conversations, the system may delete intermediary emails that are older than the final email in the collection. Be sure to assess and mark important decision emails prior to running the tool.
- ✓ Don't share personal information unless it is necessary for completing the job at hand. Keep personal information on a need-to-know basis. Share only the right information with the right person for the right purpose
- ✓ Set your Outlook to 'Show as Conversations'.



Managing your email

Commission Emails are Commission Records

Emails pertaining to the business of the commission are considered commission information, and as such, must be managed for set time periods, and possibly kept permanently.

Information schedules approved under the *Information Management Act (IMA)* provide classifications and timelines for managing all government information. Emails should only be deleted or disposed of in accordance with approved information schedules (i.e. ARCS and ORCS) and should not be subject to periodic and indiscriminate deletions.

As an employee, you are responsible for filing emails that document commission activities and decisions in the appropriate recordkeeping system (e.g. a shared drive, organized according to ARCS and ORCS).

Remember that your email account is a communications tool, not a place to manage records.

For more information on filing emails see the section on Saving Emails Outside of Outlook.

Deciding What to Keep or Delete

Do I need to keep every email? When can I delete an email?

You need to save all emails that pertain to the business of the commission, except for transitory emails. Transitory emails contain information of temporary usefulness that is needed only for a limited time, to complete a routine action or prepare a subsequent record. You may delete transitory emails when they are no longer needed.

You must not delete any emails that may be responsive to an active FOI request or request for legal discovery.

You should save emails that document an important government decision. For more information on the duty to document decisions, see the Guidelines on Documenting Commission Decisions.

Keep or Delete

Examples of official emails (that must be saved and managed):

- emails that document business transactions (initiation, authorization, or completion)
- emails that document decisions, including instructions, approvals, advice, and signed briefing notes
- emails that document a policy decision, significant action, or how a case was managed
- formal communication about commission business
- emails that contain information that is integral to a file about one event, client, or issue (e.g. a case file)
- legal advice and agreements
- unread email that is evidence of attempted consultation
- emails that contain other information that helps explain the history of a relationship, decision or project

Examples of transitory emails (which can be deleted):

- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- emails conveying an attachment (if it doesn't add value to the attachment)
- meeting arrangements
- routine correspondence about drafts and revisions
- a request to call someone
- personal emails such as lunch/coffee arrangements and birthday wishes

Decision guidance

1. Is this email needed for your work?
   (Does it provide evidence of official business, policies, actions, transaction, or decisions?)
2. Does it hold a final document not kept elsewhere in the recordkeeping system?
3. Is it a draft/revision with information on decisions/approvals not found elsewhere?
4. Is it working material essential to understanding final documents?
5. Are you the main, or only, recipient for the commission?

If the answer is yes to any of these questions, then the email should be saved.

If the answer is no to all of these questions, then you can delete the email as a transitory record.

For more information on determining if you should keep or delete an email, see our Email Decision Diagram and our Official vs Transitory Records guides.

Organizing Email in Outlook

My inbox is a mess! How can I manage all my emails?

An unruly inbox will seem daunting to many. Organizing your email inbox is fundamental for proper email management. Aim to identify and act on emails as soon as they arrive in your inbox.

This section will guide you through a number of useful tools you can use to organize and classify your emails in Outlook 2016 for Windows (some of these features may not be available for other versions of Outlook). The tools include:

- **Folders**
- **Categories**
- **Rules**

Important

When you file an email into the recordkeeping system (such as the shared drive) the original email in Outlook is redundant and should be deleted.

Not doing so may cause confusion to which version is the official or trustworthy record.

Working with Folders

It may be useful to think about email management in the context of paper practices. In the pre-internet era, messages would arrive to your office inbox in paper form. They wouldn't just stay in that inbox; you would read the messages then either file them away or dispose of them. The inbox was a temporary storage location, not a final destination. The same is true of your Outlook inbox today.

As a rule, employees should file or delete their email as soon as possible after sending or receiving them. However, this isn't always possible or desirable. Creating custom folders in Outlook to organize your inbox will help you file and delete emails in a timely manner.

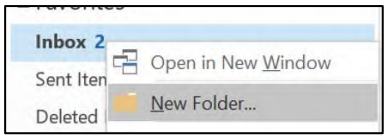
Best Practice: It is recommended that you create Outlook folders according to classifications in information schedules (i.e., ARCS and ORCS). Use the file code (ARCS and ORCS primary and secondary numbers) in the folder name. Create a folder for each project you are working on or create a subject-based folder. Create as many sub-folders as you need. If you decide this, contact Records and Information Services for assistance with ARCS and ORCS.

If that seems like too much right now you can get halfway there and set up folders for specific topics or parts of your job, and that will still put better order in your Outlook.

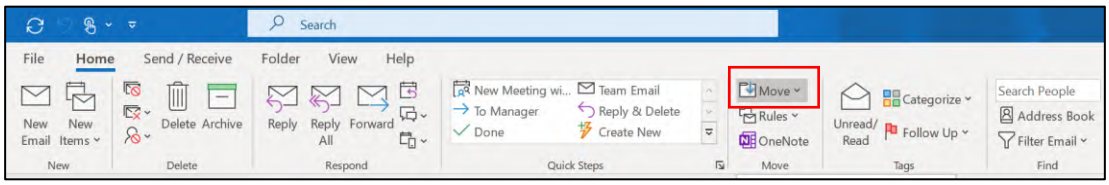
It is also good practice to create a transitory email folder for items that are of temporary usefulness. You can apply rules to the transitory folder to delete transitory emails after a specified period has elapsed. See the section on Deleting Emails Appropriately.

To create a new folder:

1. Right-click the Inbox folder in the navigation pane and choose New Folder. Type the new folder name and press Enter.



2. Drag and drop messages from your Inbox into the new folder, or, use the Move button to move the email into a folder (you can pick from a drop-down list of recently used folders)



Working with Categories

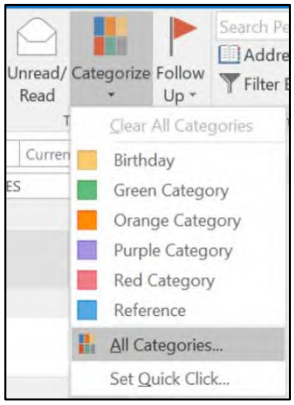
Colour Categories in Outlook are another useful way of organizing your inbox. Not only do colour categories allow you to visually identify your emails at a glance, but you can use them to perform quick sorts, populate search folders and much more.

Outlook has a number of default categories which have been named according to their colour. You can customize them to categories that make sense to you.

1. Click the Categorize button in the upper ribbon to open the list of categories.

2. At the bottom of the drop-down list, choose the option to view all categories. In this pane you can add or delete categories, or rename them according to your preference. Choose categories that work for you, such as Action, To Read, etc..

3. Go back to your Inbox, click on the email to highlight it, then click on the Categorize button again, to select the category from your list (right clicking on the email also brings up the Categorize option).



Working with Rules

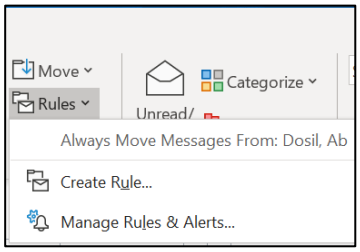
Rules can be useful for automatically moving email to a specified folder. If there are specific people, subjects, categories, or topics that will always go in the same folder, you should set up a rule that automatically routes those emails to that folder.

To set rules:

1. Click on the Rules button in the upper panel to open the drop-down menu.

2. Select Manage Rules and Alerts.

3. In the Email Rules tab, select New Rule. This will allow you to choose from a number of rule templates that you can customize, or you can create your own rules from scratch using the Create Rule.



Saving Email Records Outside of Outlook

A recordkeeping system is a shared filing system in which records, including government emails, are managed in accordance with approved information schedules. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and on-going training, constitutes an appropriate system for managing government information.

An appropriate recordkeeping system should:

- contain logical, organized naming conventions that can be followed by all staff;
- ensure the preservation and accessibility of records over time;
- protect against accidental or unauthorized access, alteration, copying, movement or deletion;
- minimize duplicate storage of records; and
- permit the retention requirements of information schedules to be applied accurately and efficiently.

This section will provide guidance on how to save emails to your office's recordkeeping system. It will walk you through:

- **Saving email – responsibilities**
- **Tips for saving email records**
- **Preferred email preservation formats**
- **Locations for saving emails**

Saving Email – Responsibilities

Managing email is the responsibility of every employee

It is the responsibility of all staff to manage their emails appropriately. You should identify emails that are records of your business activity, move them out of your Outlook mailbox, and manage them alongside related records in your office's recordkeeping system.

The email sender is responsible for saving internal email

It is the responsibility of the sender of an email or the initiator of a dialogue to decide if the email and/or attachment(s) constitute an official record. If the email or its attachment(s) contain key decisions and/or actions taken, it should be considered a record, renamed (if appropriate), and saved in the most appropriate place.

The principal receiver is responsible for saving external email

If you are the sole recipient of an external email or, if there are several recipients, and you are responsible for the most relevant work area, you are responsible for deciding if the message forms part of an official record or not and taking responsibility for its management.

Working groups should assign responsibility for shared mailboxes

When managing emails in a shared mailbox, working groups should be clear as to who is responsible for the retention, naming, capture and disposal of emails within the mailbox. Without the identification of clear responsibilities, emails may be lost or duplicated. It is recommended that the folder owner take responsibility for a shared mailbox.

Tips for Saving Email Records

A complete record includes sufficient content, context, and structure to ensure that the information can be accessed, understood, and preserved for as long as necessary, and that its value as evidence will be maintained. To do this, you need to preserve all elements of the email, including the email header, the message body, and any attachments.

- To prevent a loss of information, move emails to an appropriate location as soon as possible.
- It is not necessary to capture every email in an email conversation thread separately. Instead emails should be captured at key points during the conversation, when key decisions are made and transactions processed.
- Email attachments should be saved as part of the record to provide context to an email. However, there will be occasions when it won't be necessary to capture both the email

and its attachment. For example, if an attachment has been sent for reference purposes and you know it has been captured elsewhere.

- If the title of the email does not accurately reflect the content of the message then it should be re-titled at the point at which it is saved. Renaming email records is particularly important when they represent different points in an email string as it will identify the relevant aspects of the conversation.

- Consider dating the email in the title before saving it. For government bodies who receive a high volume of requests under FOIPPA, the ability to sort by date is particularly important. Use the format YYYY-MM-DD to date your emails in the title.

Preferred Email Preservation Formats

For filing on the Shared Drive: .MSG

MSG files are the native Outlook format. When you drag and drop an email to your desktop or to a LAN folder, this is the file format that is exported. Outlook can export calendar items, emails, contacts, and other Outlook content via MSG. This format is preferred because all header information, message content and attachments are preserved with the file. The file will retain a lot of its original functionality when reopened.

For filing anywhere (ideal for long-term storage): .PDF

Emails can be exported from Outlook by printing them to a standard PDF file or a PDF portfolio. PDF files are stable and generally well supported, making them the de facto preservation standard for documents. The Adobe PDF conversion plug-in is available when you download Adobe Acrobat. This allows for one- click conversion of Outlook content to PDF.

You can also save attachments embedded in a PDF, just like an email; however, this method can cause compatibility issues. Best practice is to download the attachment and save it with the email content to ensure it can be opened in the future.

Saving Email Records on Your Shared Drives

Saving email to a shared folder on your office Shared Drive network is our best option until we have an EDRMS. To do this, simply:

- Copy and paste the email from your Outlook to the shared folder. This will save it as an MSG file.
- Right click on the message and click Properties.
- Check the Read-Only box, click Apply and OK. This will ensure that the message cannot be edited by others.
- You can also save your emails as PDFs on a shared drive folder. Saving email PDFs and their attachments separately is recommended. While it is possible to embed the attachment within the PDF, this method is not stable and attachments can be difficult to open later. The ability to open and inspect attachments is critical for proper email preservation.

Deleting Email Appropriately

Now that you know what constitutes an official email record and how to save them properly, you should delete the redundant (duplicate) emails from your Outlook. You are also encouraged to delete transitory emails, personal emails and other non-record reference material that is taking up valuable space.

Deleting emails quickly and appropriately ensures that your inbox will remain clean and clutter-free.

This section will provide guidance on simple Outlook tools that will help you to delete your emails appropriately. It will also include simple exercises you can perform to find and delete common categories of transitory email.

Tools include:

- **Clean-up Tool**
- **Auto-delete Folders**
- **Assign Policy for transitory emails**
- **Empty Deleted Items on Exit**
- **Exercise: Find and Delete Emails to Distribution Lists**
- **Exercise: Find and Delete Meeting Requests**

NOTE: You are prohibited at all times from 'triple-deleting' emails (i.e. attempting to purge an email from your 'Recover Deleted Items' folder).

This should not be confused with double deletion, which happens when deleted emails are cleared from the 'Deleted Items' folder. The double deletion process is important for clearing

space in your Outlook account, but must only be done if the items in question are permitted to be disposed of.

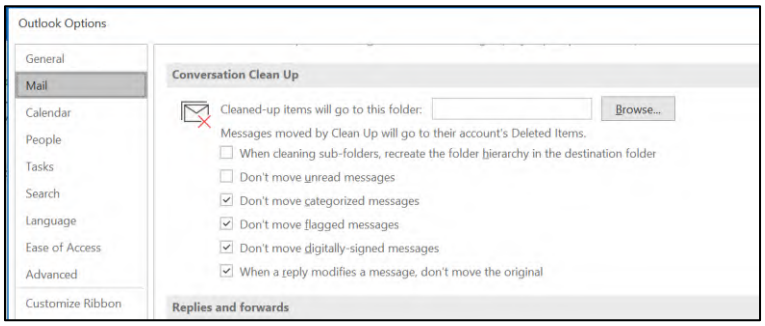
Working with the Clean-up Tool

Email threads (termed “conversations” in Outlook) can be long and cumbersome. As people reply to the email thread, the existing content is automatically included in each response, resulting in a lot of redundant information. The Clean Up tool scans conversations and removes any redundant emails from the thread.

Before cleaning up a conversation, ensure that important emails are flagged or categorized.

To set the parameters of the Clean Up tool:

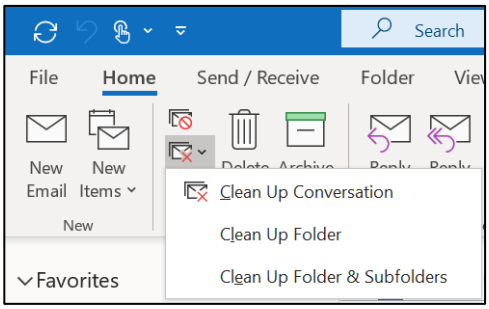
1. Click File, then Options.
2. In the Outlook Options pop-out window, select the Mail tab on the left and scroll down to Conversation Clean Up. By default, all cleaned up items will go to the Deleted Items folder. You can change this destination folder if you would like them to be routed elsewhere. There are options that allow you to prevent certain classes of email from being cleaned. Ensure that flagged emails and categorized emails are not cleaned.



To run the Clean Up tool:

1. Highlight the folder you would like to clean. Click Clean Up.
2. From the dropdown menu, there are 3 options: run the clean up tool on a single folder; on a folder and its subfolders; or on specific conversations.
3. It is recommended that you run the conversation cleanup tool regularly as part of your work routine.

   Use caution with this tool, and refrain from cleaning email threads that may contain important information.

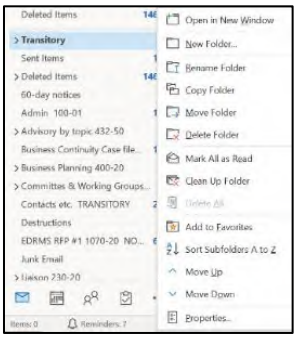


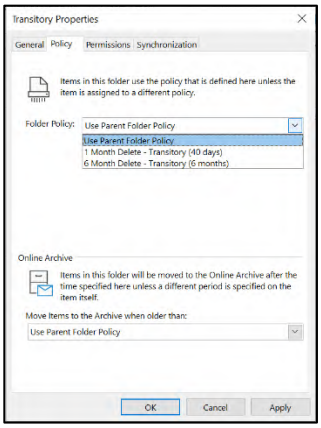
Working with Auto-delete Folders

As mentioned in the section on Folders, setting up a Transitory Folder is recommended to keep your inbox clear. You can set Outlook Rules to auto-route certain classes of transitory emails directly to this folder. There is also the option of configuring this folder to permanently delete transitory emails after a specified period. Automating this process encourages you to think critically about what is transitory and what is an official record.

To configure this setting:

1. Highlight your Transitory Emails folder in the left navigation pane, and right click on the folder to open the drop down menu.
2. Select Properties.
3. In the pop-out window, select the Policy tab.
4. In the drop down menu beside Folder Policy, select the term for how long you want your transitory emails to remain in the folder. One month is recommended. Click OK. Your transitory email folder will now auto-delete items that are older than one month.



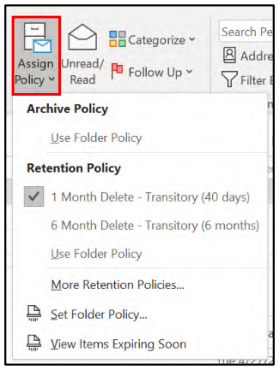


Working with Assign Policy tool

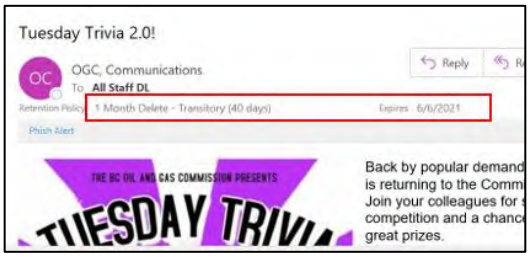
You can also assign an auto-delete policy to individual transitory emails right in your inbox or other folders. This will permanently delete the selected emails after a specified period. When you do this, think about the value of the record - whether it is transitory or an official record - and once you assign the policy, you don't have to think about it again.

To apply the policy directly to an email:

1. Select the transitory email and click on the Assign Policy button.
2. Choose the retention you prefer for the email from the picklist.



3. Notice the email now states your chosen retention period, with the “expires” (deletion) date. When the email reaches the expiry date it will be automatically deleted, and moved to your Deleted Items folder.



NOTE: Once a retention policy is applied, you cannot remove it. If you change your mind and need to retain the email for longer you can click on Assign Policy and extend the retention to the 6 month option. Also, if you save the email to a folder on the shared drive, the transitory retention will be removed.

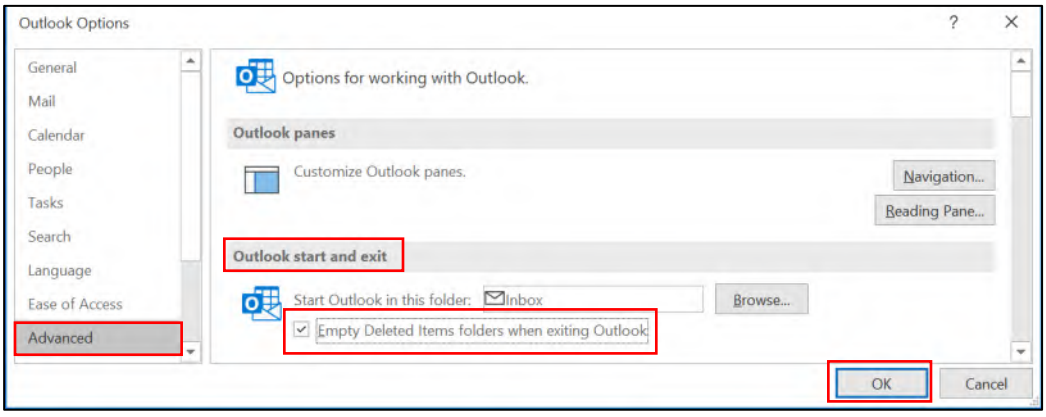
If an FOI or legal matter arises your transitory records are within search parameters, and your auto-deletion will be suspended until the matter is closed.

Emptying Deleted Items on Exit

Clicking Delete in Outlook does not permanently delete the email; it sends it to the Deleted Items folder. In the default settings, this folder will not be emptied unless you do so manually. However, you can configure Outlook to empty your Deleted Items automatically when you exit the application. This is the recommended option.

1. Click File, then Options.

2. Choose the Advanced tab on the left side. Under the “Outlook start and exit” heading, check the box that says Empty Deleted Items folder when exiting Outlook and press OK.

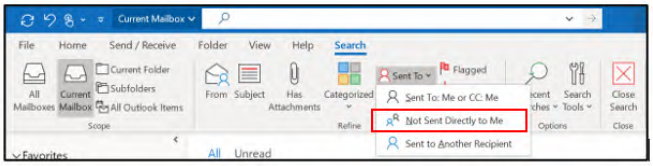


Exercise: Find and Delete Emails from Distribution Lists

Emails received through internal distribution lists are another type of transitory email. As the receiver, you are generally not responsible for filing emails received through a distribution list (although you may want to keep a copy for reference purposes). To find and delete all emails that are not sent directly to you:

1. Click the search bar to open the Search tab and menu.

2. Select Sent To, to open a dropdown list. Click on Not Sent Directly to Me. This should return all emails sent through distribution lists.



   Always exercise caution before deleting large quantities of email.

Related Policies

- ✓ Employee Code of Conduct and Ethics
- ✓ Information Management Policy
- ✓ Information Security Policy
- ✓ Mobile Device Policy
- ✓ Use of IT Resources Policy
- ✓ Workplace Appropriate Use Policy

Contacts

If you would like more information regarding this guide please refer to the table below.

Commission Contact	When to Contact	Email
Records and Information Services (Records Management) MyOGC Information Management Page	For inquiries on how to manage government information.	servicedesk@bcogc.ca
Records and Information Services (FOIPPA and Privacy) MyOGC FOI Page	For general inquiries, or to report a privacy breach.	FOIintake@bcogc.ca
IT Service Desk Service Desk	For technical support or ensuring your mobile device is encrypted.	servicedesk@bcogc.ca
Cybersecurity MyOGC Cybersecurity Page	For general inquiries, or to report an incident of phishing, cybersecurity attacks, or a data breach.	servicedesk@bcogc.ca
Human Resources MyOGC Human Resources (HR) Page	For general inquiries about the Code of Conduct and Ethics.	servicedesk@bcogc.ca

Appendix A: Managing Phishing and Spam Quarantine

We all have a role to play in protecting the Commission and our information assets. Here are some tools our cybersecurity team has implemented to help protect us from malicious email activities.

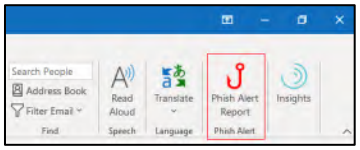
Managing Phishing Emails

If you receive an email that that you consider to be a phishing or other cybersecurity threat, you need to report it by using Phish Alert in Outlook. Reporting an email using the Phish Alert tool will delete the email and send a copy to Cybersecurity for analysis.

While we are transitioning to M365 you will see either of these two actions for reporting a suspicious email:

1. Click on the Phish Alert banner at the top of your email, or

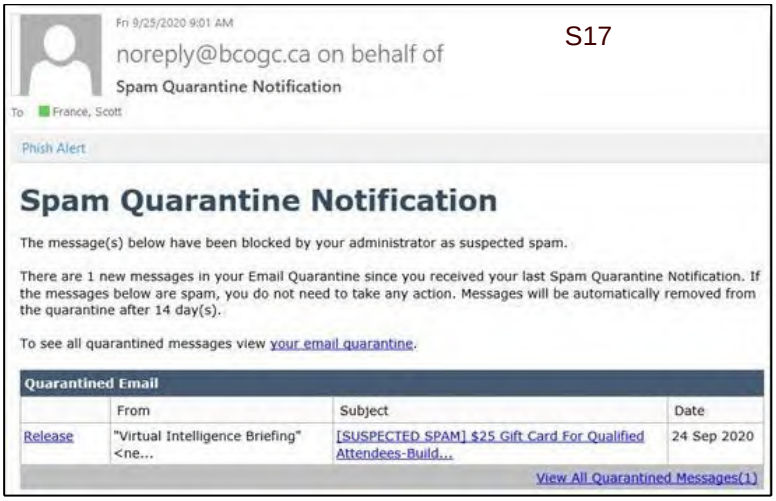
2. Click the Phish Alert Report button located on the Home toolbar.



Both actions will report the email as a potential malicious email, and quarantine it by removing it from your Inbox.

Managing Spam Quarantine Notifications

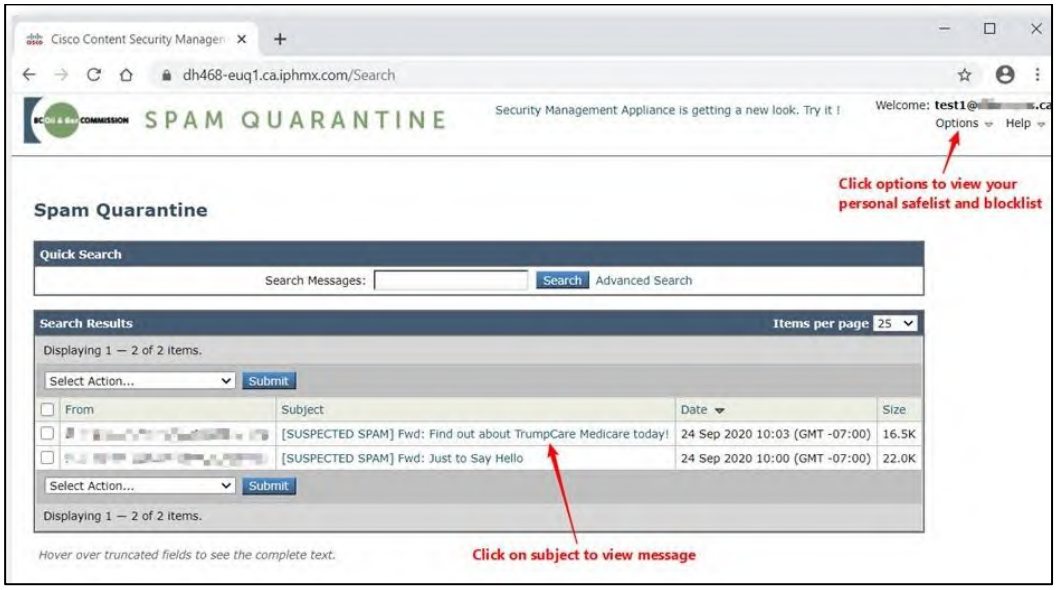
On occasion you may receive email notification of an email that has been moved into your spam quarantine. If an inbound email is suspected of being spam, our spam filter will move it to quarantine, rather than deleting it, and you will receive this notification email in the next business hour.



S17

Hover your mouse over the links, and note the not so user-friendly domain name **dh468-euq1.ca.iphmx.com** the links point to. This is safe and will bypass the Second Chance confirmation popup when you click links in Spam Quarantine Notification emails.

To get more information about the quarantined message, click on the View All Quarantined Messages. There is no need to sign in as authentication is done using a custom URL. This also means that staff working with shared mailboxes can manage the spam quarantine for the shared account.



Clicking on a message will allow you to safely view the body of the email so you can decide which action to take.

Message Actions:

Release – Sends email to your Outlook inbox. **Only release emails that you believe are safe!** You can always email S17 to help determine the validity of an email.

Release and Add to Safelist - Sends email to your Outlook inbox and adds senders address to your personal safe senders list.

Delete – Deletes email from your spam quarantine (this also happens automatically when the message is 14 days old).

Going to **Options** will allow you to navigate to your **SafeList** or **BlockList.** Shown below is the SafeList. Any entries here are for you only. If you feel a sender's email address should be on the SafeList for the entire Commission please contact S17

The BlockList functions in the same manner as the SafeList but blocks emails from the sender instead of allowing.

If you are unsure whether to block or allow future emails – do nothing! Future similar emails will likely just end up in the quarantine again and you may be able to make a better-informed decision.

If you want to go back and manage your SafeList and BlockList you will need to find a previous Spam Quarantine Notification email and use the links. Remember that emails in the Spam Quarantine older than 14 days are automatically deleted.

CHIEF RECORDS OFFICER DIRECTIVE ON DOCUMENTING GOVERNMENT DECISIONS

DIRECTIVE:	CRO 01-2019
SUBJECT:	**Documenting Government Decisions**
AUTHORITY:	This directive is issued under section 6 of the *Information Management Act.*
APPLICATION:	This directive applies to all government bodies.
EFFECTIVE DATE:	March 31, 2019

Chief Records Officer

Directive to Government Bodies
issued under section 6 of the *Information Management Act*

Under section 6 (1) of the *Information Management Act*, S.B.C. 2015, c. 27, I, Joel Fairbairn, Chief Records Officer, issue the following directive respecting documenting government decisions.

Creating an appropriate system

1. The head of a government body must, in ensuring that an appropriate system is in place within the government body for creating and maintaining government information that is an adequate record of that government body's decisions, take reasonable steps to ensure that the government body complies with this directive and is guided by any guidelines issued under section 6(1) of the *Information Management Act*.

Elements of an appropriate system

2. An appropriate system must include at least the following:
    a. recorded policies and procedures and defined roles and responsibilities for creating and maintaining, in a manner consistent with this directive and any applicable enactments and provincial government policies, adequate records of decisions that the head of the government body has determined, in accordance with this directive and any guidelines issued under section 6(1) of the *Information Management Act*, are to be recorded;
    b. appropriate recordkeeping systems that ensure the preservation and accessibility of records of decision over time;
    c. a program for ongoing training of relevant employees of the government body respecting the creation and maintenance of adequate records of decisions;
    d. a program for monitoring implementation by the government body of the system and of its compliance with applicable laws and government policies.

Determining which decisions are to be recorded

3. The head of a government body, in determining which decisions of that government body are to be recorded, must consider whether a record of decision would:
    a. inform the government body or others about the evolution of the government body's programs, policies or enactments;
    b. protect the legal or financial rights or obligations of the government body, the Crown, or any person, group of persons, government or organization that is directly and materially affected by the decision;
    c. facilitate the government body's accountability for its decisions, including through internal or external evaluation, audit or review.

Adequate records of decisions

4. Government information is an adequate record of the government body's decision if it can reasonably be expected that someone not familiar with the circumstances in which the decision was made could be reasonably informed about the following, as applicable:
    a. the individual who made the decision and that individual's title;
    b. when the decision was made and when it takes effect;
    c. any person, group of persons, government or organization reasonably likely to be directly and materially affected by the decision and, where practicable, the way in which they are reasonably likely to be affected by the decision;
    d. the basis for and context in which the decision was made, including, as applicable, any relevant legal, policy or factual information.

Other obligations

5. This directive does not affect any statutory or other legal obligation for a government body to create or maintain a record of decision or other government information.

This Directive is effective as of March 31, 2019. It remains in effect until rescinded or superseded.

March 21, 2019
Date

Chief Records Officer

CHIEF RECORDS OFFICER GUIDELINES ON DOCUMENTING GOVERNMENT DECISIONS

Purpose

These guidelines assist government bodies in meeting their obligations under the *Information Management Act* (IMA) related to documenting their decisions.

Government bodies must refer to these guidelines and CRO Directive 01-2019 (Directive) in considering whether their practices are sufficient to meet the obligations under the IMA. The Chief Records Officer (CRO) may provide further guidance on documenting decisions of government bodies, as necessary or appropriate.

Why Document Government Decisions?

- Supports openness and transparency
- Facilitates effective decision making
- Preserves corporate memory
- Supports employees in doing their jobs effectively and providing high-quality services to the public
- Supports accurate reporting of decisions to stakeholders, including other government bodies and the public
- Contributes to the Province's historical record for future generations

Application

These guidelines apply to all British Columbia government ministries and any government agencies designated as "government bodies" under the IMA.[1]

Other government agencies not currently covered by the IMA may use these guidelines as a best-practice tool.

These guidelines do not limit any other statutory or legal requirements respecting the creation or maintenance of records of government body decisions, or any other government information.

Background

Section 19 (1.1) of the IMA requires that government bodies have an appropriate system in place for creating and maintaining government information that is an adequate record of their decisions.[2]

The Directive sets out the components of an appropriate system for creating and maintaining government information, and what constitutes an adequate record. These guidelines expand on the Directive. Together, the Directive and these guidelines provide a principle-based framework that government bodies are to operationalize in a manner suitable to their respective mandates. Government bodies should ensure that they can demonstrate compliance with the IMA, the Directive and these guidelines.

[1] http://www.bclaws.ca/civix/document/id/loo102/loo102/109_2016

[2] Section 19 (1) of the IMA also stipulates that the head of each government body is responsible for ensuring that an appropriate system is in place within their organization for managing and securing government information. This directive does not provide information or advice about the appropriate system for managing and securing government information.

All government bodies are expected to have the appropriate combination of people, processes and technology in place to ensure that government information is created, held, transferred, archived and disposed of in accordance with the IMA. This includes adequate records of decisions.

The head of a government body must consider these guidelines and the Directive in ensuring that they have an appropriate system in place.

As part of good government and accountable public administration, government has policies, processes and procedures in place to support the appropriate creation and maintenance of government information in accordance with the IMA.

The Government Records Service (GRS) within the Corporate Information and Records Management Office (CIRMO) is available to assist government bodies in meeting their information management obligations, including those related to adequately documenting their decisions.

Getting Started

Identifying and Documenting Decisions

Step 1: Ascertain whether the decision needs to be documented under the IMA (Appendix A)

Step 2: Determine whether the current practice will result in an adequate record of the decision (Appendix B)

Ensuring an Appropriate System is in Place

Consider whether the prescribed elements of an "appropriate system" are in place within the government body (Appendix C)

Addressing Identified Gaps

If necessary, conduct a gap analysis and identify remedial actions

Identifying Decisions that Should Be Documented

Government bodies do not have to create and keep records of every decision made by every employee. Government bodies need to identify which decisions are to be documented by applying their judgement, in the context of their specific mandates and with consideration to the purpose and intent of the IMA, the Directive and these guidelines, and other obligations that may exist in law and policy respecting documenting decisions.

To help determine if a decision is required to be documented under the IMA, refer to the attached decision flowchart in Appendix A and to these guidelines.

A government body should document a decision where a record would serve one or more of the following purposes:

- Informing the government body or others about the evolution of the government body's programs, policies or enactments;
- Protecting the legal or financial rights or obligations of the government body, the Crown, or any person, group of persons, government or organization that is directly and materially affected by the decision;
- Facilitating the government body's accountability for its decisions, including through internal or external evaluation, audit or review.

Line of Business Decisions

In assessing which line-of-business decisions are to be adequately documented under the IMA, government bodies must bear the above purposes in mind. Government bodies also should document statutory decisions and decisions respecting a course of action that directly and materially affects a person, group of persons or organization.

Often, documenting decisions made by Senior Executive (i.e., Deputy Minister or equivalent, Assistant Deputy Minister or equivalent), members of the Executive Council, administrative tribunals or other quasi-judicial decision makers will meet the above purposes. There will, however, be circumstances where, in order to adequately document line-of-business decisions in light of the above purposes, a government body will document decisions made outside Senior Executive.

Common Corporate Decisions

Common functional areas where decisions are typically documented according to generally accepted policies and procedures include:

- Decisions related to preparing legislation;
- Decisions related to
    - strategic policies that define or change corporate direction, or
    - programs or initiatives to fulfill the government body mandate;
- Human resources (HR) decisions;
- Budget and other financial decisions; and
- Procurement decisions.

Adequate Records of Decisions

Government body employees must take reasonable steps to ensure that adequate records of decisions are created and maintained.

The Directive defines the elements of an "adequate record" of a government body's decision. Adherence to common corporate practices will generally support alignment with requirements to adequately document decisions. Those practices are to be considered, along with the following guidance.

In general, a record of decision is adequate if it can reasonably be expected that someone not familiar with the decision could be reasonably informed about the following, as applicable:

- Who made the decision and under what authority;
- When the decision was made and, if appropriate, when it takes effect;
- Who is reasonably likely to be directly and materially affected by the decision and, where practicable, the way in which they are reasonably likely to be affected by the decision; and
- What are the basis for and context in which the decision was made, including, as applicable, any relevant legal, policy or factual information.

Contextual Information

An adequate record of any key decision must include the material contextual information that informed the decision.

This information can be in many formats and will vary significantly depending on the nature of the decision.

Contextual information may typically be found in the following formats:

- A decision briefing note
- An application form
- An entry in a case management system or a case file
- Other records (e.g., memos, letters, emails) containing advice, recommendations and/or options
- Records of verbal advice
- Treasury Board Staff and Legislative Counsel advice to Cabinet
- Legal opinions
- Appendices or attachments that could include such things as: medical information, education information, employment information, income information, or other program-specific information that supports accountability, protects the rights or obligations of affected parties, or is otherwise necessary to understand the decision

Not all of these factors will apply to every decision. For example, many decisions do not affect others, so it is not necessary to document who is reasonably likely to be affected or how. Government bodies are expected to carefully consider, in the circumstances of each case, what is required to adequately document a decision. In some cases, an adequate record of a decision may be a note in a case management system or case file; in others it may comprise copies of extensive studies.

It is also important to remember that a record is required to be "adequate", not "perfect".

In addition, it is not necessary for a single record to be created that contains all of the material contextual information. The amount and type of contextual information that is adequate will vary depending on the nature of the decision.

Adequate Records of Common Corporate Decisions

Statutory Decisions

Government bodies will generally have existing policies and guidance on documenting relevant statutory decisions. In general, an adequate record of a statutory decision should include a statement setting out the specific decision in the form of a directive, order, authorization or permit, confirmation of eligibility for a benefit or service, etc. Other material contextual information (such as the decision's legal authority), and reasons for the decision, may be required.

Decisions Related to Preparing Legislation

Adequate records must be created during every step of preparing any enactment, including Bills, regulations and ministerial orders. This includes initial information gathering and analysis, developing a request for legislation, and the drafting process.

Before a government body's policy initiative can proceed to a proposal for legislation and the drafting stage, a substantial amount of information must be gathered and assessed. Cabinet Operations provides detailed information on requirements for Cabinet decision documentation, and the Office of Legislative Counsel provides information on the preparation of drafting instructions. These requirements are to be complied with.

Decisions About Government Body Policies and Programs

Decisions that establish, change or terminate corporate direction, or programs or initiatives to fulfill the government body's mandate, should be documented. Adequate records of decisions related to establishing, changing or terminating policies or programs must include a record of decision (e.g., any one or more of an approved decision note or a Cabinet or Treasury Board submission, as applicable).

HR Decisions

The BC Public Service Agency (BCPSA) maintains detailed guidance for ministries on documenting various HR decisions. This includes guidance on hiring, managing attendance, illness and injury, and taking disciplinary actions. Government bodies must comply with BCPSA guidance on documentation of HR-related decisions.

In the absence of similar policies, government bodies that are not subject to the *Public Service Act* may wish to use the BCPSA guidance as a model to determine what constitutes an adequate record of decisions related to HR matters.

Budgeting and Other Financial Decisions

The Core Policy and Procedures Manual (CPPM) Chapter 3: Planning, Budgeting and Reporting covers all aspects of government financial management, including documentation. Government bodies must comply with CPPM Chapter 3 in relation to documentation of financial management decisions.

Government bodies not subject to CPPM will generally have their own financial policies that address documentation. They may use CPPM Chapter 3 as a model to determine what constitutes an adequate record of decisions related to budgeting and financial decisions.

Procurement Decisions

Government bodies regularly make decisions regarding various types of procurement, including goods purchasing, contractor services and information management/information technology procurement. CPPM Chapter 6 covers all aspects of government procurement and states that ministries are responsible for "planning, managing and fully documenting the process to acquire goods, services and construction." Government bodies must comply with CPPM Chapter 6 in relation to documentation of procurement-related decisions.

Government bodies not subject to CPPM will generally have their own procurement policies that address documentation but may also use CPPM Chapter 6 as a model to determine what constitutes an adequate record of decisions related to procurements.

Appropriate System for Creating and Maintaining Records of Decisions

The IMA requires each government body to ensure that an "appropriate system" is in place for creating and maintaining records of decisions.

The Directive defines the elements of an appropriate system for creating and maintaining government information that is an adequate record of a government body's decisions. An appropriate system must include the components discussed below. To help determine if you have an appropriate system for creating and maintaining decisions, refer to the following guidance and to the flowchart in Appendix C.

Many aspects of an appropriate system are already addressed under the corporate information management framework, which comprises information management legislation (including the IMA, FOIPPA and their regulations), ministerial orders and ministerial or CRO directives, and, for ministries, CPPM Chapter 12: Information Management and Information Technology Management. The entirety of this information management framework should be considered when creating and administering an appropriate system consistent with the Directive and these guidelines.

What Is an "Appropriate System"?

An "appropriate system" for documenting government decisions is about more than technology. It includes policies, processes, roles, responsibilities and controls necessary to ensuring that adequate records of decision are created and maintained.

Defined Roles and Responsibilities

The CRO has a statutory mandate under the IMA to provide leadership, direction and oversight, and to promote effective information management across government bodies. GRS is the central organization responsible for records management, including developing policies, guidelines, standards and training to assist government bodies in identifying appropriate information schedules, establishing recordkeeping systems, and ensuring records are preserved and accessible as required and appropriate.

Section 19 (1.1) of the IMA stipulates that the head of each government body is responsible for ensuring that an appropriate system is in place within their organization for creating and maintaining, in accordance with applicable CRO directives or guidelines, government information that is an adequate record of that government body's decisions.

To support the overarching governance structure for an "appropriate system", government bodies should clearly define roles and responsibilities for information management within their respective organizations. This can include designating staff to champion and promote information management within their program areas. Such staff should be at a sufficiently senior level and have relevant knowledge and skills. They should also have clear authority, and clear, committed and ongoing Senior Executive support, respecting all aspects of information management (including documentation of decisions).

However, it is also important to recognize that employees at all levels actively manage government information in the course of their daily work. Accountabilities should be clearly articulated to assist government bodies in meeting their business goals and to ensure that legal obligations are met. All program area staff should have a clear understanding of their roles and responsibilities for documenting decisions.

Some decision making is formally or informally delegated. Some examples of formal delegations of decision making include:

- delegations to government body expense authorities;
- persons delegated any of the director's powers, duties or functions of a Minister or official under an act. (Some laws require these delegations to be in writing.)

Some responsibilities will be established more informally, such as through job descriptions, training, policies or procedures, or even through system design and workflows.

For example, a government body employee may be responsible for preparing a briefing note for decision by a Senior Executive about a significant public policy matter. They may have the delegated authority to make a decision about an individual's eligibility for a program, service or benefit. The same employee may be entitled to make spending decisions up to a certain dollar amount, and may be accountable for making and keeping records related to HR matters for their direct reports. No matter how the accountability is delegated or assigned, the government body's policies, procedures and training should make it apparent to each employee what their accountabilities are with respect to creating and maintaining adequate records of government decisions.

Common Types of Government Body Recordkeeping Systems

- Structured Local Area Network (LAN) with the Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS) applied, as appropriate
- Enterprise Document and Records Management System (EDRMS)
  - EDRMS Content Manager (formerly TRIM) is the government standard
- Line of business applications (e.g., case management systems)
- Hardcopy (paper) filing systems

Documented Policies and Procedures

As noted earlier, a robust high-level information management framework already exists for ministries. This corporate framework comprises information management legislation such as the IMA, associated regulations, CRO directives, as well as CPPM Chapter 12. Non-ministry government bodies may use the existing corporate framework as a foundation for their own policies and procedures.

Each government body knows its own lines of business best and is therefore best placed to develop organization-specific policies and procedures regarding an appropriate system for creating and maintaining information.

Government bodies create records for many different legislated, policy and operational reasons. Government bodies should consider identifying what policies, procedures, training and awareness activities, and compliance and monitoring tools are already in place with respect to documenting their decisions. This will enable them to determine if gaps exist or changes to their existing approach are needed. When changes are required, the government body is best placed to develop its own specific policies and procedures to establish and operate an appropriate system for creating and maintaining information, including adequate records of decisions.

Appropriate Recordkeeping Systems

Government information must be created and maintained in accordance with corporate records management policy and standards. This applies to the creation and maintenance of adequate records of decisions.

An appropriate recordkeeping system should:

- contain logical, organized naming conventions that can be followed by all staff;
- ensure the preservation and accessibility of records over time;
- protect against accidental or unauthorized access, alteration, copying, movement or deletion;
- minimize duplicate storage of records; and
- permit the retention requirements of information schedules to be applied accurately and efficiently.

Information schedules describe and classify government information and specify how long information must be kept. They are approved by the CRO under the IMA[3] and set out the final disposition of a record (i.e., whether it will ultimately be transferred, archived or destroyed). By law, if no information schedule applies, the information must be held until the CRO approves an information schedule or the information's transfer, archiving, or disposal. If a government body does not have an approved information schedule, it should document internal policies and procedures for ensuring information is retained as appropriate in light of the nature and content of the information.

Training and Awareness

All employees need to have a clear understanding of their responsibilities related to creating and maintaining government information, including records of decisions. At a minimum, ministries must ensure employees take mandatory information management training (e.g., IM 117: Information Management: Managing government information, privacy, access to information and security). CIRMO has also prepared materials for all government bodies to support them in complying with their obligations respecting creating and maintaining government information that is an adequate record of government body decisions. There may be also be government body- or sector-specific training appropriate to some roles and responsibilities. This includes the appendices to this directive, training, and more.

[3] Any "record schedule" approved by the Legislative Assembly under the *Document Disposal Act* between 1936 and 2016 is continued under the IMA.

Compliance Monitoring

Government bodies should proactively monitor and assess their activities, practices and processes to ensure that they are meeting expectations respecting the creation and maintenance of government information. This includes the creation and maintenance of adequate records of decision. This will help ensure their organizational needs are met and that the government body is compliant with the Directive, these guidelines, and applicable policy and law.

CIRMO's Information Management Practice Review Program works with ministries to facilitate self-assessments of their information management practices, including the obligations in the IMA respecting documenting government decisions. CIRMO will also conduct practice reviews to assess the maturity of the information practices implemented by ministries to foster the continuous improvement of those practices. Other public bodies subject to the IMA may wish to use this tool to monitor and assess their own activities.

Contact Information

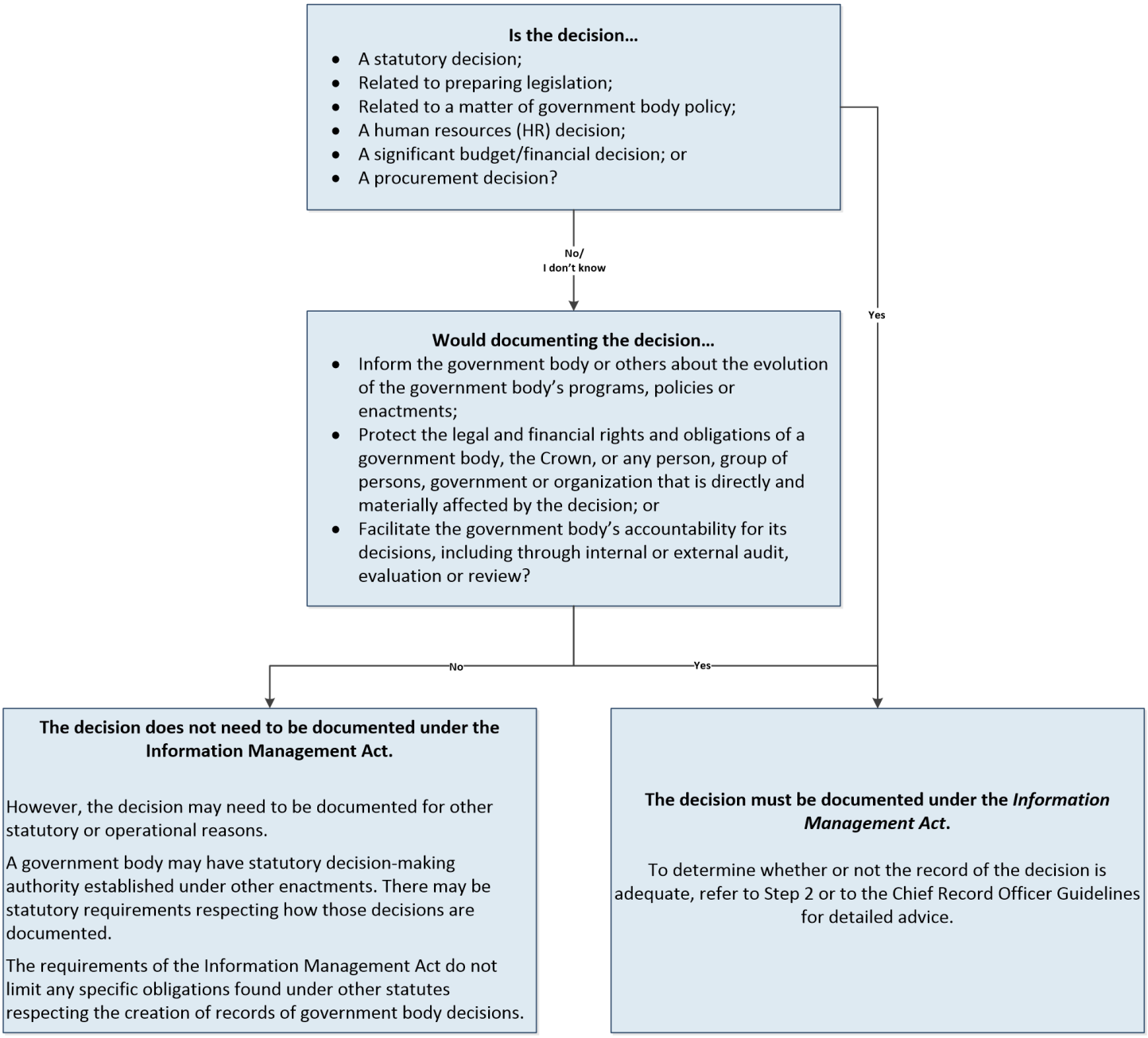
Government Records Service
Corporate Information and Records Management Office
Ministry of Citizens' Services

Email: GRS@gov.bc.ca

Appendix A

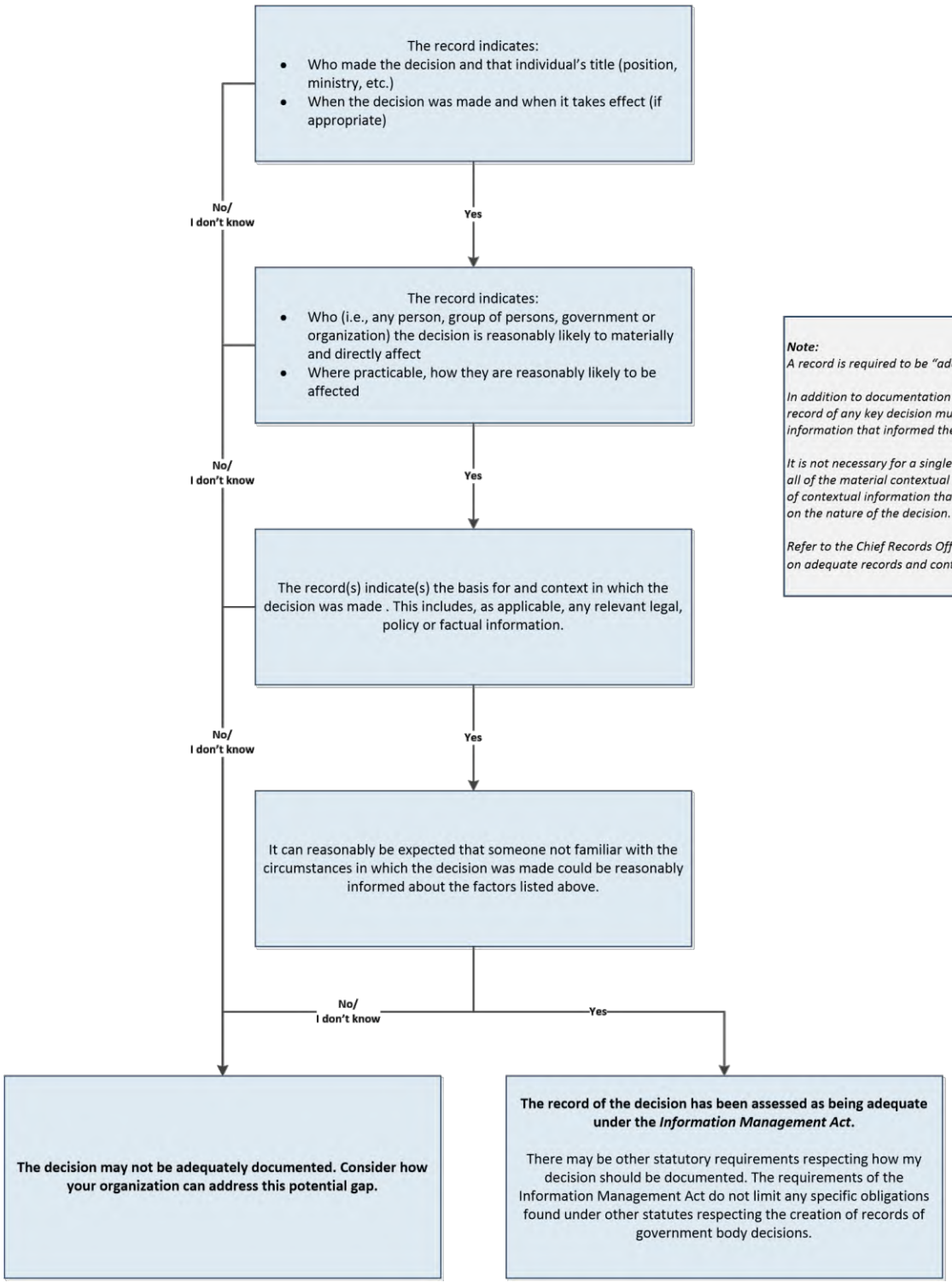
Identifying and Documenting Decisions

STEP 1: Does a Decision Need to Be Documented Under the *Information Management Act*?



Identifying and Documenting Decisions

STEP 2: Is the Record of a Decision Adequate Under the *Information Management Act*?



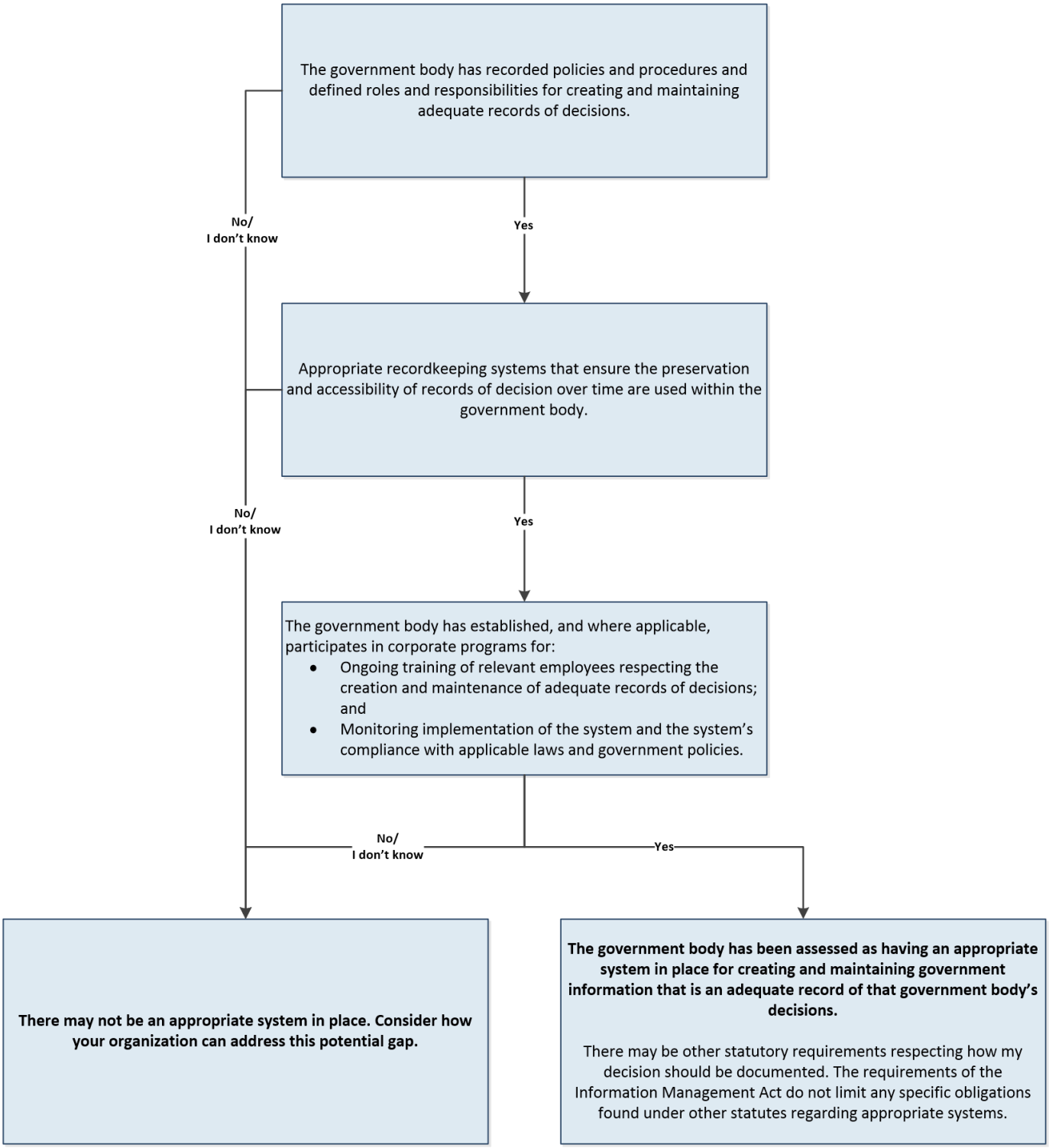
Note:
A record is required to be "adequate", not "perfect".

In addition to documentation of the decision itself, an adequate record of any key decision must include the material contextual information that informed the decision.

It is not necessary for a single record to be created that contains all of the material contextual information. The amount and type of contextual information that is adequate will vary depending on the nature of the decision.

Refer to the Chief Records Officer Guidelines for further advice on adequate records and contextual information.

Is there an Appropriate System in Place?



Appendix D: Additional Resources

- **Core Policy and Procedures Manual (CPPM)** combines government-wide financial policy, management policy and financial administration procedures into a single online resource: https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy
- **The Managing Government Information Policy** sets out ministry obligations for managing government information, specifically as they relate to IMA requirements: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/government-records
- **The Records and Information Management Manual (RIMM)** provides guidance to support ministries in all aspects of managing, protecting, and accessing government information, including data and records: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/government-records/rim-manual
- **The Appropriate Use Policy** establishes the policy requirements that all government employees must follow when accessing and managing government information and using information technology resources: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/appropriate-use-policy/appropriate_use_policy.pdf
- **IM 117: Information Management: Managing government information, privacy, access to information and security** is a mandatory online course for all government employees available through the BC Public Service Learning Centre.
- **ARCS and ORCS User Guide 2018 (Version 3.0)**: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-management/arcs_orcs_user_guide.pdf
- **ARCS**: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules/arcs
- **ORCS**: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules/orcs
- **Information Schedules**: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules
- **A Guide to Legislation and the Legislative Process in British Columbia – Part 1: The Legislative Process**: https://www.crownpub.bc.ca/Content/documents/1-LegislativeProcess_August2013.pdf
- **Hiring Documentation (BC Public Service Agency)**: https://www2.gov.bc.ca/gov/content/careers-myhr/hiring-managers/process/documentation

Documenting Commission Decisions

Mahia Frost & Josh Christensen

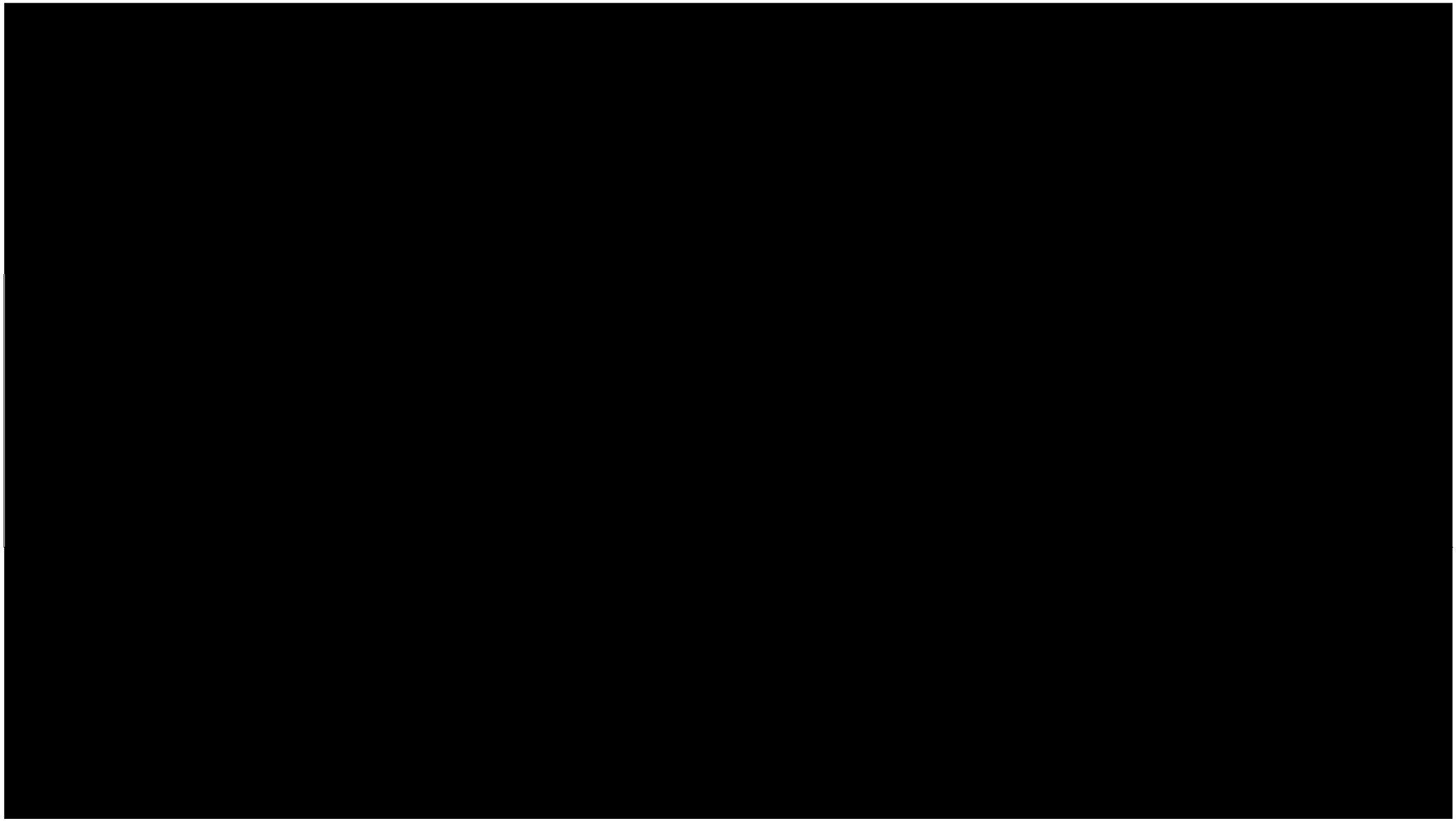
June 2019

BC Oil & Gas COMMISSION

Objectives of the Workshop

- Learn about legislative changes to documentation of government decisions
- Discuss how those changes apply to the Commission
- Apply tools to help you comply with the changes
- Wrap up & next steps

Who Likes Videos?



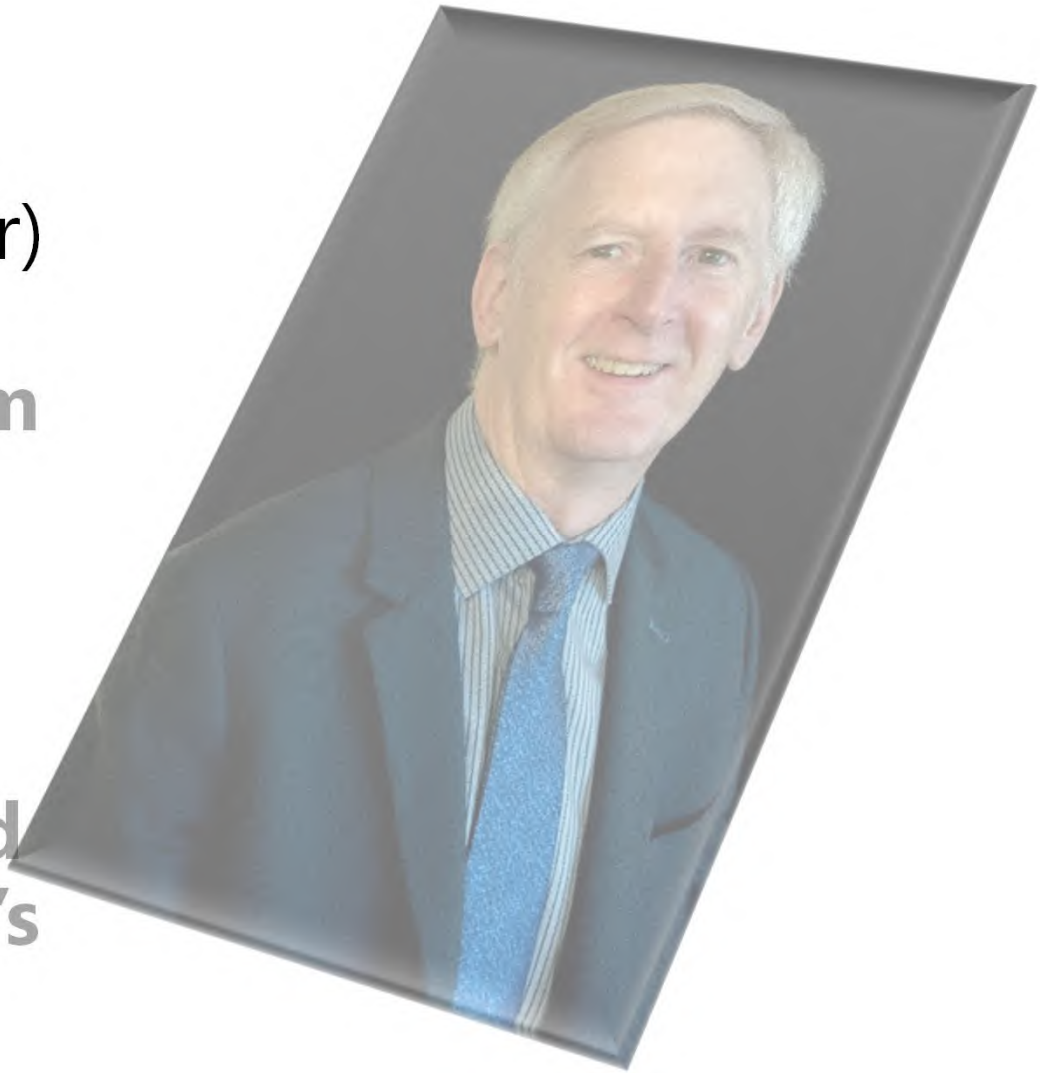
Legislative Changes

- Bill 6, *Information Management (Documenting Government Decisions) Amendment Act*, introduced in 2017
- Changes from this legislation came into force March 31, 2019
- Information Management Regulation of the IMA designates the Commission as a government body subject to it

Why Changes Apply to the Commission

According to the *Information Management Act*:

- The head of a government body (i.e. the Commissioner) is responsible for ensuring that **an appropriate system** is in place within the government body for **creating and maintaining government information that is an adequate record of that government body's decisions**



How Changes Apply to the Commission

Why Do Changes Apply to You?

What to Document: A Framework

- What decisions are “key”?
- How can we make sure decisions are adequately documented?
- Where are the documents kept?

Tools that Help

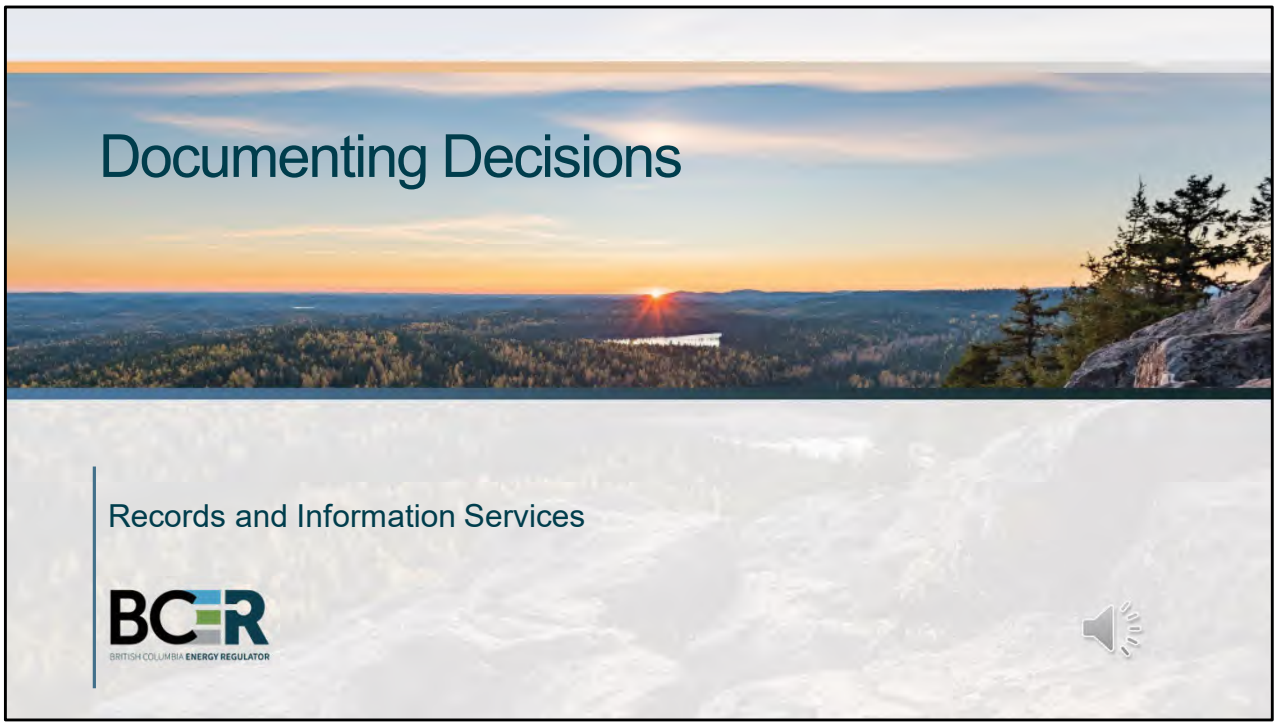
- Documenting Commission Decisions Checklist: Three Steps
  1. Is it a decision that needs to be documented?
  2. Is the documentation adequate?
  3. Is there an appropriate system in place?

- Documenting Commission Decisions Process Chart
  – See posters in the room

Workshopping It

- Workshop session 1: Decision Brainstorm
  - What decisions do you make both routinely and periodically?
- Workshop session 2: Decision Analysis
  - Do you need to document the decision?
- Workshop session 3: Adequacy Analysis
  - Is the decision documented adequately?

- Mahia Frost
  Specialist, EDRMS & Information Management Solutions
  Mahia.Frost@bcogc.ca
  250-419-4423

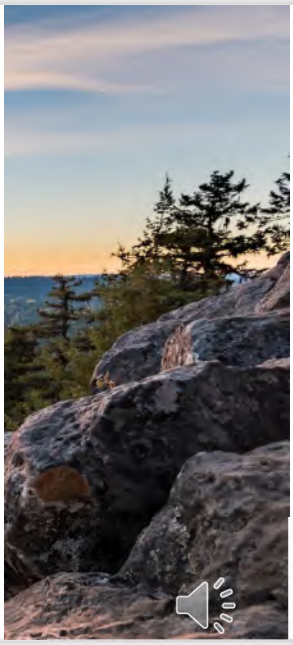


Welcome to a learning session on documenting decisions, presented by Records and Information Services.

Objectives

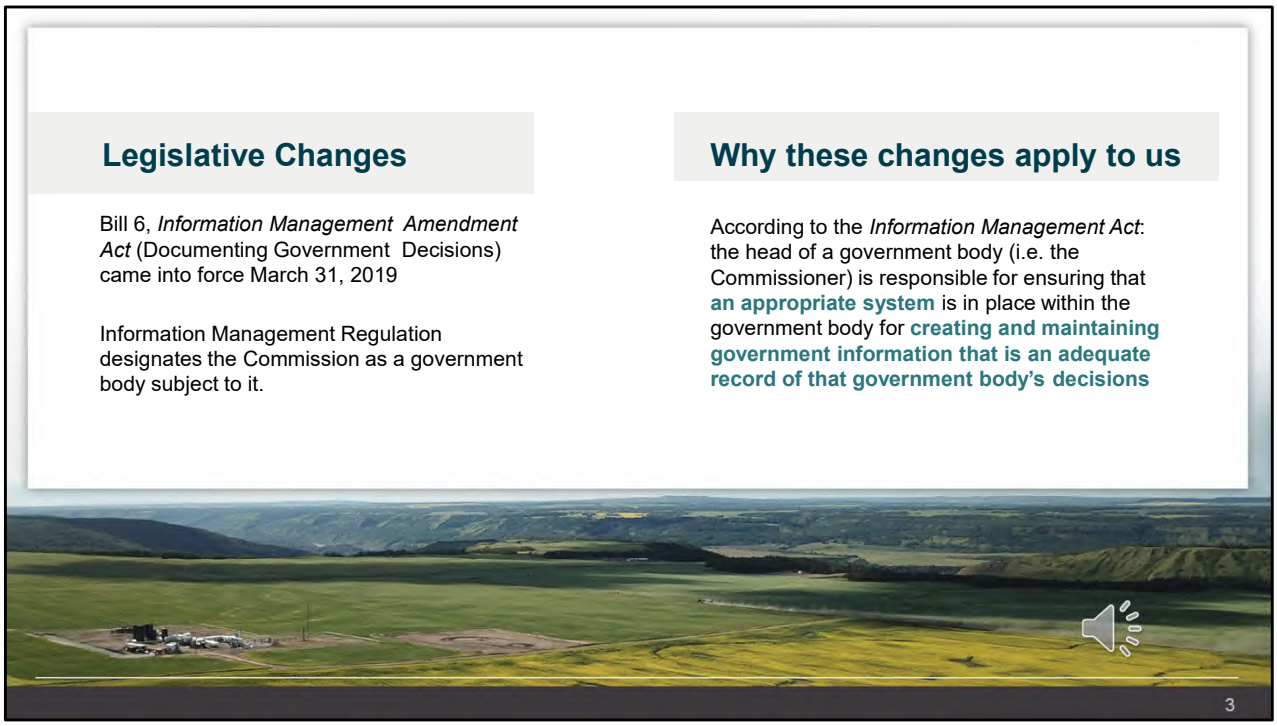
Learn about legislative requirements to document decisions

Understand how this applies to our organization

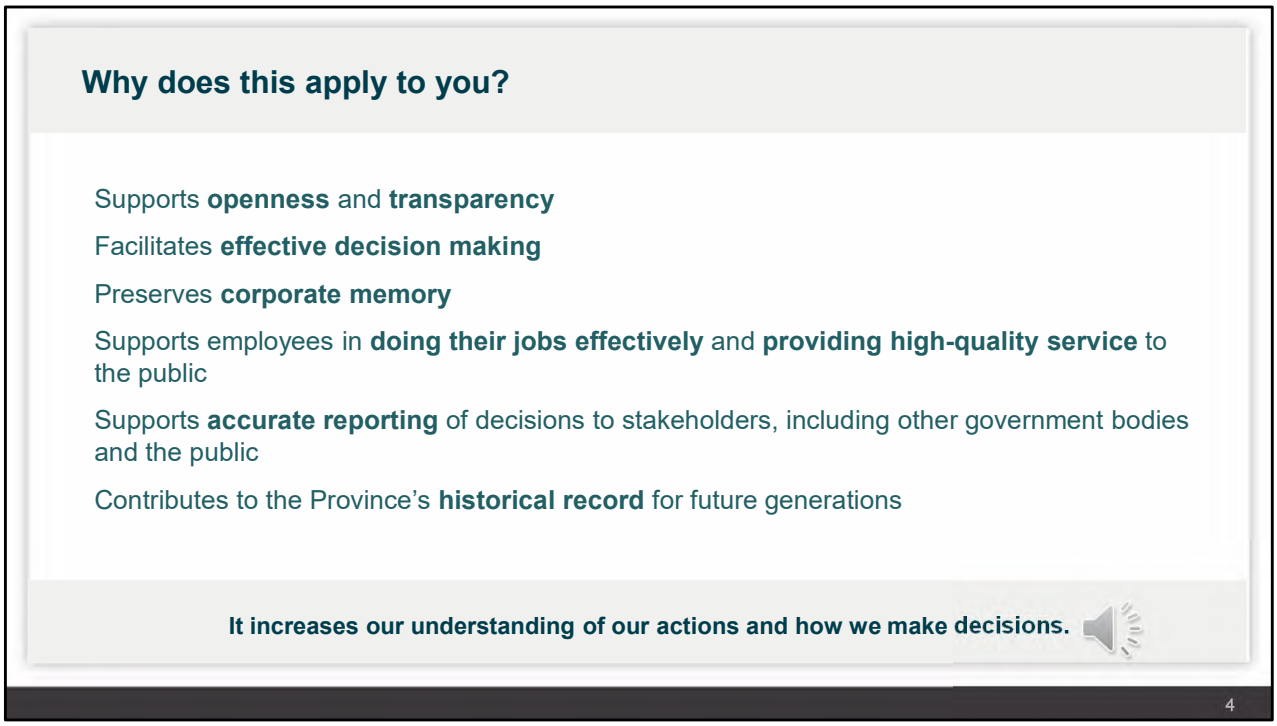


2

Today we are going to learn about legislative requirements to document our decisions and understand how this applies to our organization

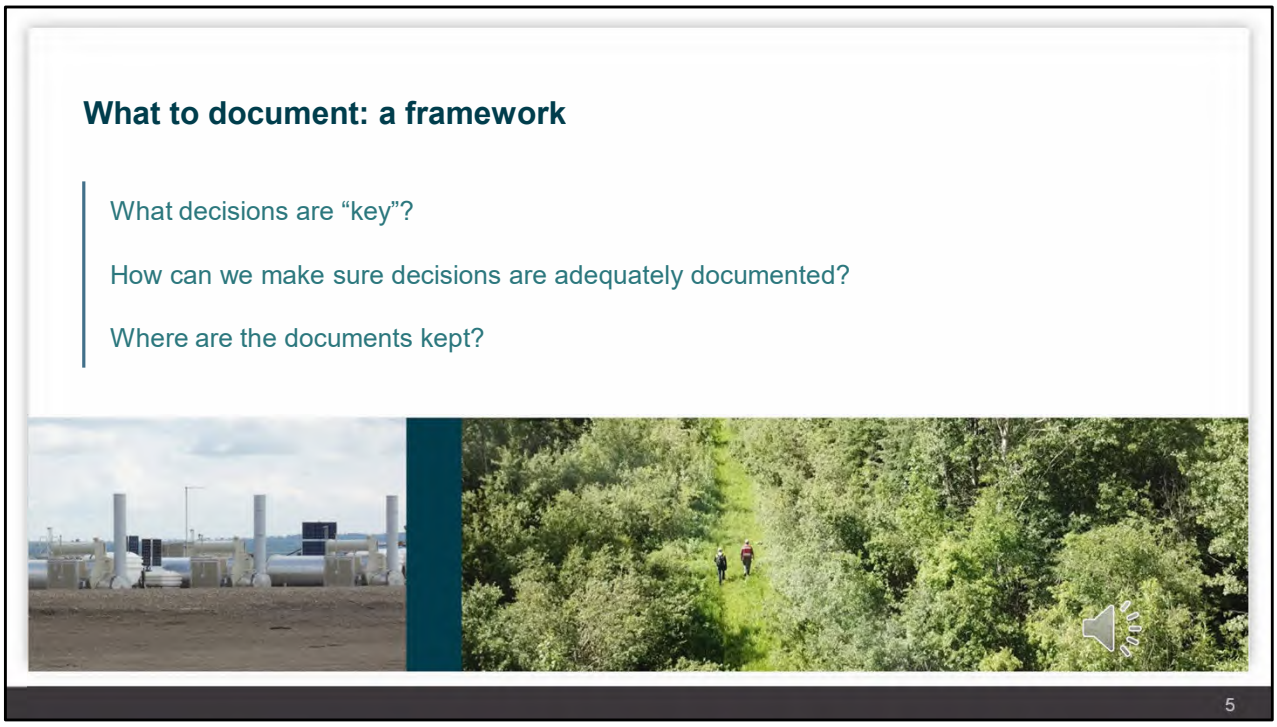


In 2019 the provincial government adopted a legislated requirement under the Information Management Act (the IMA): a requirement to ensure we are adequately documenting government decisions. While this has long been considered a best practice, embedding this in legislation makes it a corporate accountability and legislative compliance matter. Key words in this slide that we are talking about today: We are going to **talk about the concept of an appropriate system**, how to identify **the decisions we need to record**, and about **what an adequate record is**. <NEXT SLIDE>



This **is** good practice. Ensuring we keep a record of our key decisions supports our transparency initiatives, aids effective decision making, preserves our corporate memory, and helps us do our jobs more effectively. It also supports accurate reporting to stakeholders
and provides context for our actions as a government and regulatory body.
This applies to everyone, and there are many practical reasons to document decisions – so we can understand:

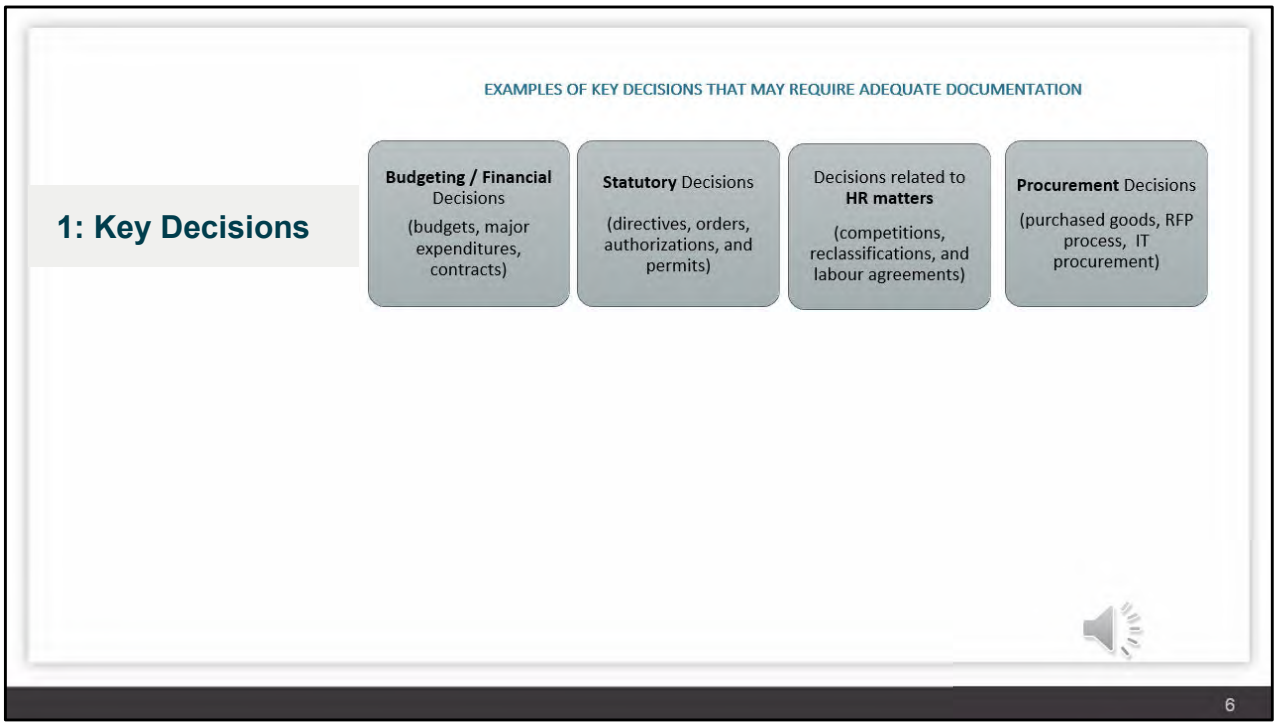
- Why they decided to cancel that project
- What did we consider last time we were faced with a decision like this
- What do people need to know about how we got to this decision and
- Helps new employees know how we make decisions <NEXT SLIDE>



The documenting decisions framework is broken down into 3 steps:

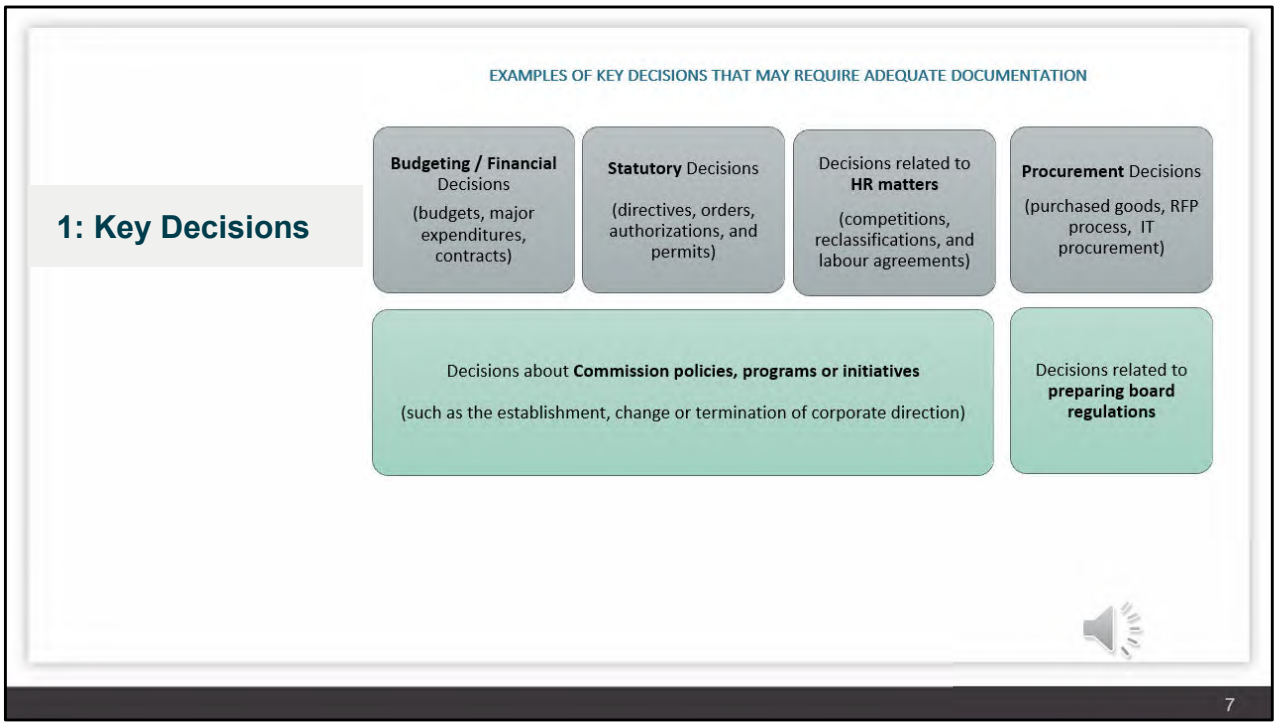
1. Identify the key decisions that we need to create a record of – or, document.
2. Determine whether the record of the decision is adequate, and
3. Make sure that the people who need to refer to those decisions can find the record of them

As BC Energy Regulator employees, we make decisions every day,
some minor, some significant.
The decisions you make depend on the services you provide and the work that you do.
For example, in the Regulator, we hire people, we assess industry applications, we create e xternal audit programs, and we develop systems that support our workflow, and we all make some sort of decisions while carrying out these functions.
The focus here is on whether we are adequately documenting our **key** decisions. We do not need to create records of every decision.
We can apply our professional judgement to identify which should be documented and determine how best to prepare adequate records of those decisions. <NEXT SLIDE>

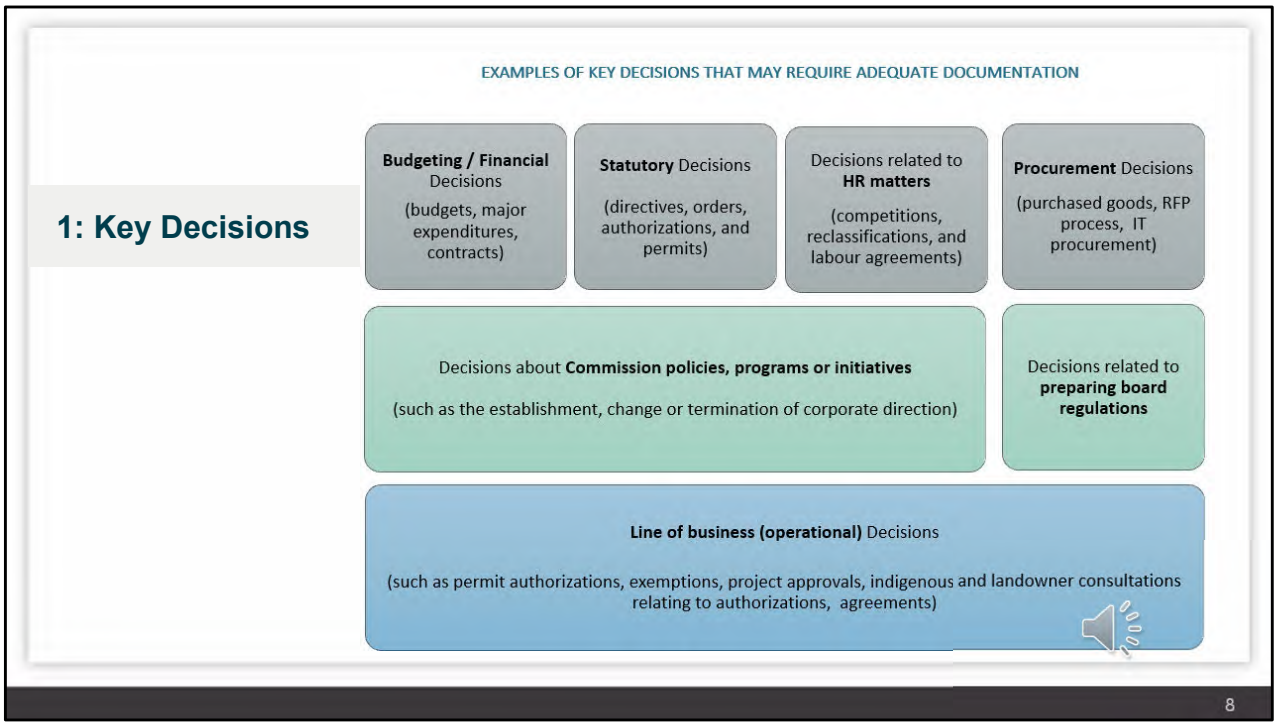


Let's talk about categories of decision that are Key under the Information Management Act:

The first category is the Protection of legal or financial rights or obligations. This is important because it's about protecting people's rights and financial transparency. For the example of a grant, why we decided to grant money, or why we didn't. <NEXT SLIDE>



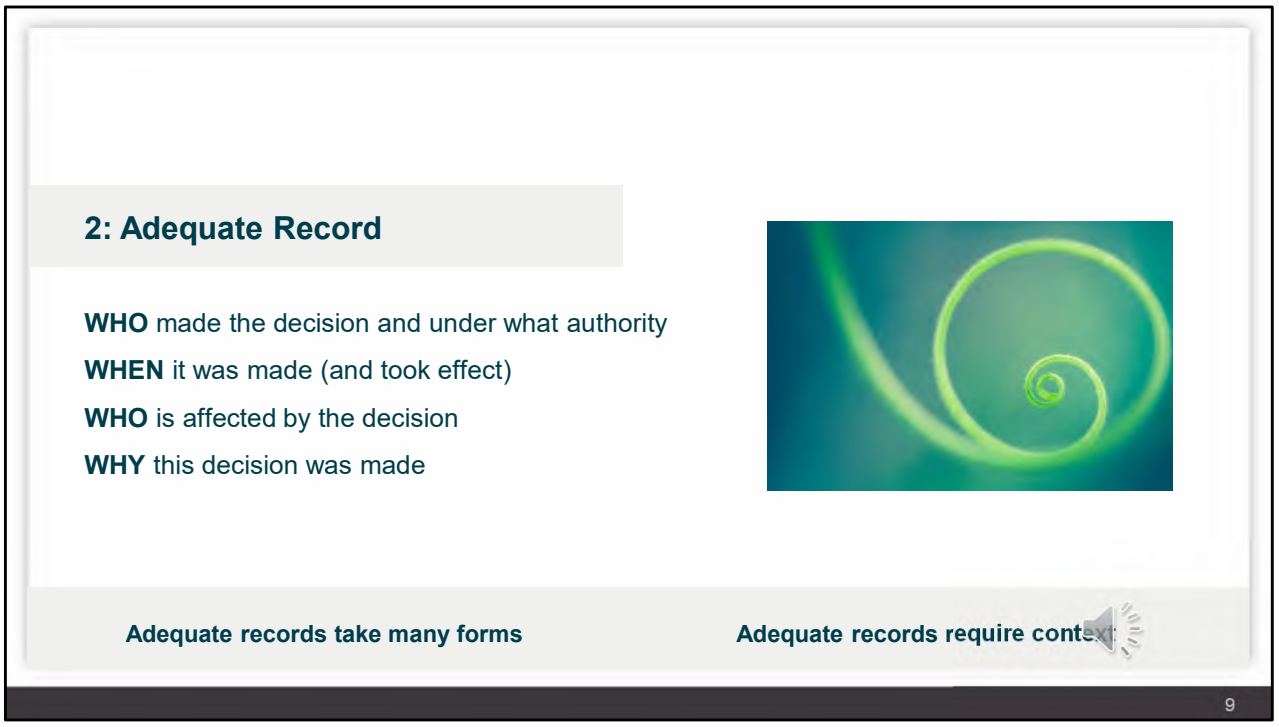
The next is to document the evolution of our programs, such as why a grant is created, or the creation of our orphan program or our compliance management information system. <NEXT SLIDE>



And to Facilitate accountability. The "Think like a citizen" consideration – what would they want us to record about why and how we created the orphan program. What will help us be accountable for our business decisions. You will see in the slide that many of our operational decisions fall under this. The IMA guidelines identify decision types common to most organizations, but then each one, ours most certainly, make many decisions under the authority of our own regulatory framework and we want to be sure we keep an adequate record of those.

A good point here is also that

Documenting decisions made by Senior Executive will often meet our purposes. <NEXT SLIDE>

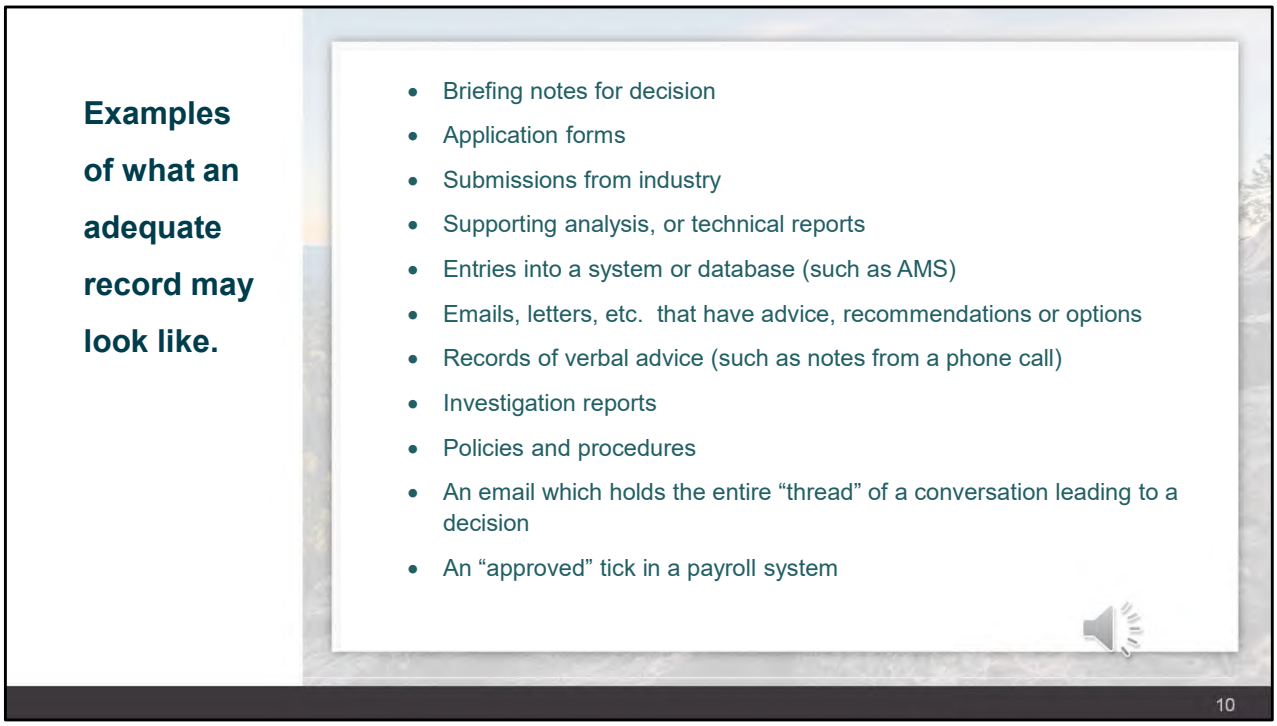


When we know what our key decisions are, we need to be sure we retain an adequate record of them. When we talk about an adequate records we simply mean – is the record enough.

A record of decision is adequate if someone who is not familiar with it could determine:

- **Who** made the decision, and under what **authority**
- **When** the decision was made (and took effect)
- **Who** is likely to be affected by the decision
- **What** is the basis for the decision, and context in which the decision was made (such as relevant legal, policy or factual information that was on hand at the time)

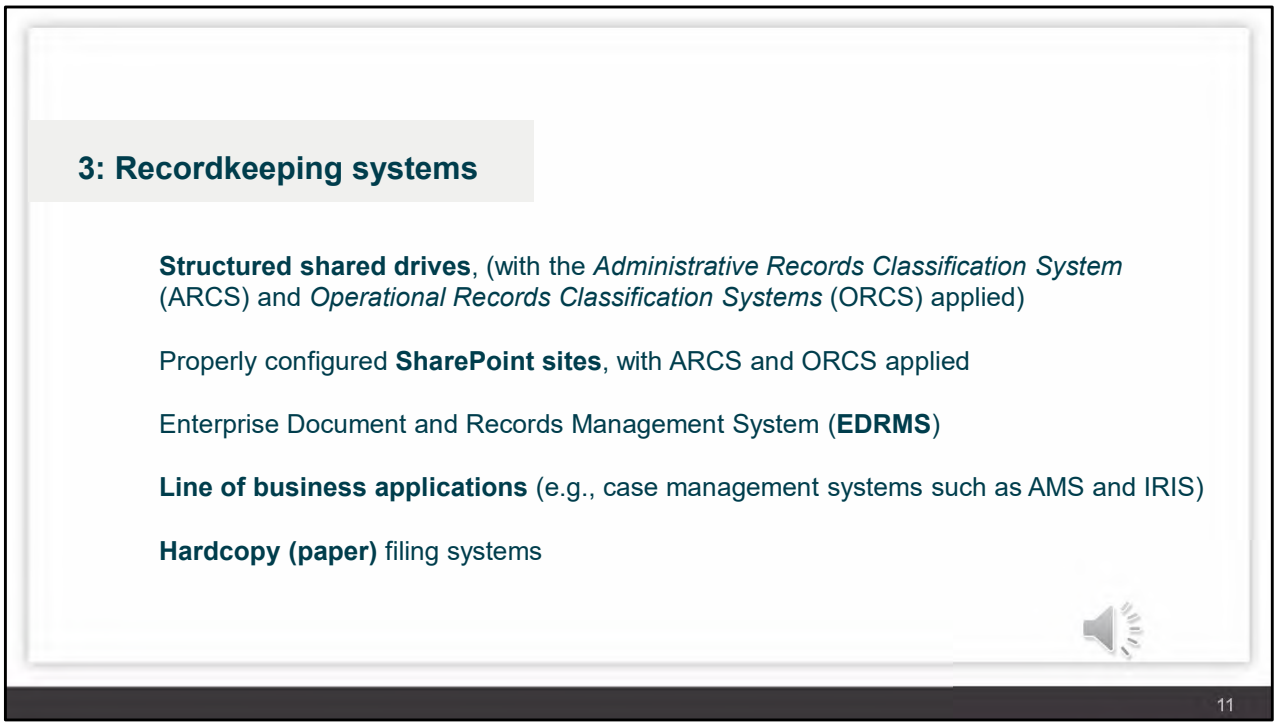
Not all of these factors will apply every time, but ask yourself: Could someone who wasn't familiar with the decision understand it?
There are many "persons who are unfamiliar" – this could be future you / FOI requester / Litigation teams or your team in your absence while on holidays. <NEXT SLIDE >



Here are some examples of what an adequate record may look like
<small pause>
You will notice that Adequate records take different forms, and this will vary depending on the decision. In some cases, an adequate record of a decision may be a note in a file, or a one-page form. Other decisions may be supported by thousands of pages of analysis and advice. The record of decision should be proportionate to the nature, impact and importance of the decision.

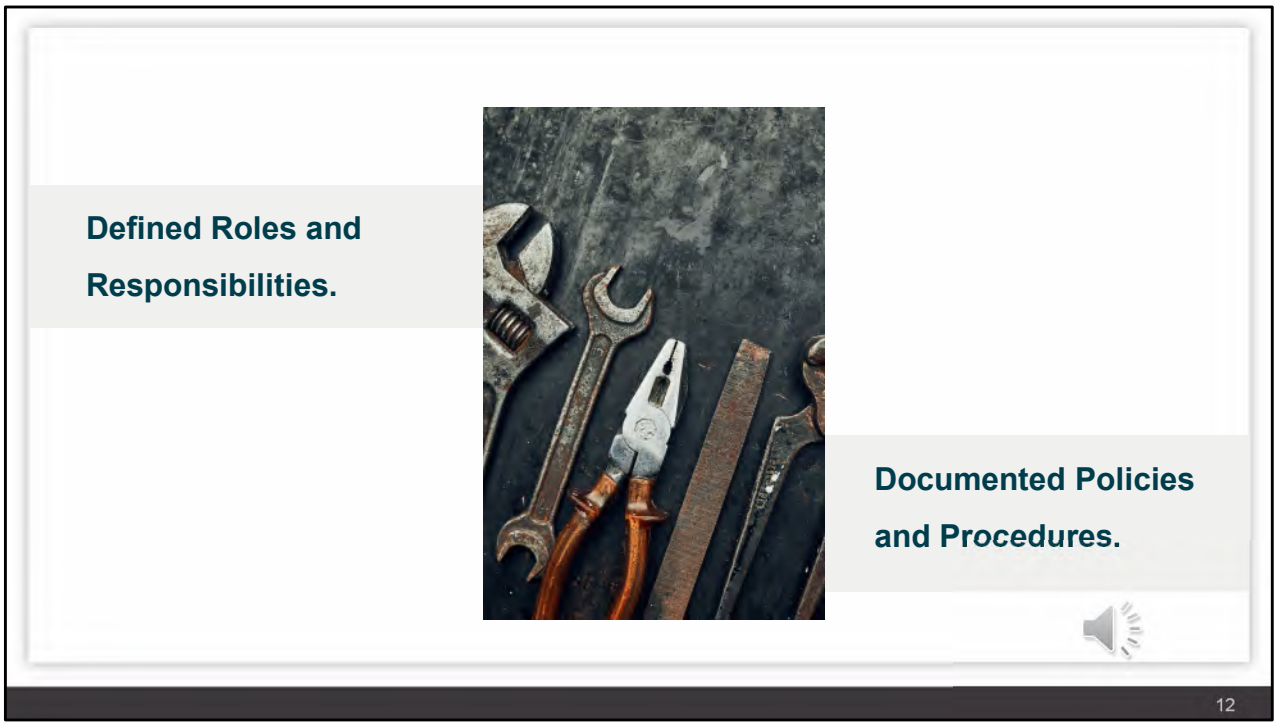
Also, adequate records include **context**.

An adequate record is more than just the "decision" itself. We want to be sure that the context for the decision is part of the record. Remember, our goal is for a person unrelated to the original decision-making process to understand who made it, why it was made, and what information it was based on. <NEXT SLIDE>



The third element of this requirement is that we have an appropriate system in place for creating and maintaining records of decisions. . They use the phrase an “appropriate system”. This is not about technology. It is about the management system in place, which include policies, processes, clear roles and responsibilities, and the controls necessary to ensure the appropriate management of information.

You have determined you create adequate records of decision – are the records being managed? Are they in a central place for your team, so they can find them when they need them? Because this is also about findability. If they are in your F drive, your OneDrive or your outlook, nobody else can access them. Having those records in the branch recordkeeping system means if Brad is on holidays Joel can put his hands on a contract decision. And if Kathryn is away, Julie can figure out which requests are open and where they are in their process.
You may have been part of a shared drive organization project recently – this is part of the ongoing work to create centralized recordkeeping systems, so each branch knows where to find their records, where to file emails, documents, and records of decision, and to support us managing the records through their lifecycle. Namely, to meet this requirement. <NEXT SLIDE>

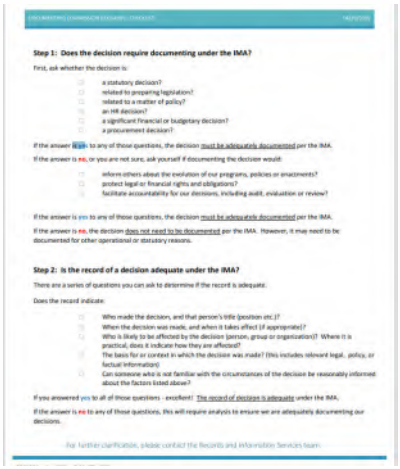


The other element of the system is to have your policies and procedures, roles and responsibilities in place, and all staff to have a clear understanding of them.
Decision making responsibilities may be formally or informally delegated. Formal delegations of decision making include expense authorities or delegated powers, duties or functions under an act.
Some responsibilities will be established more informally, such as through job descriptions, training, policies or procedures, or even through system design and workflows.
For example, a person may be responsible for preparing a briefing note for decision. They may have the delegated authority to decide about an individual's eligibility for a program, service or benefit. The same employee may be entitled to make spending decisions up to a certain dollar amount and may be accountable for making and keeping records related to HR matters for their direct reports.
No matter how the accountability is delegated or assigned, our policies, procedures and training should make it apparent to each employee what their accountabilities are with respect to creating and maintaining adequate records of government decisions. <NEXT SLIDE>

Tools to help:

Documenting Commission Decisions Checklist: Three Steps

Documenting Commission Decisions Process Chart



Step 1: Does the decision require documenting under the IMA?

First, ask whether the decision is:

- a statutory decision?
- related to preparing legislation?
- related to a matter of policy?
- an HR decision?
- a significant financial or budgetary decision?
- a procurement decision?

If the answer is yes to any of those questions, the decision must be adequately documented per the IMA.

If the answer is no, or you are not sure, ask yourself if documenting the decision would:

- inform others about the evolution of our programs, policies or enactments?
- protect legal or financial rights and obligations?
- facilitate accountability for our decisions, including audit, evaluation or review?

If the answer is yes to any of those questions, the decision must be adequately documented per the IMA.

If the answer is no, the decision does not need to be documented per the IMA. However, it may need to be documented for other operational or statutory reasons.

Step 2: Is the record of a decision adequate under the IMA?

There are a series of questions you can ask to determine if the record is adequate.

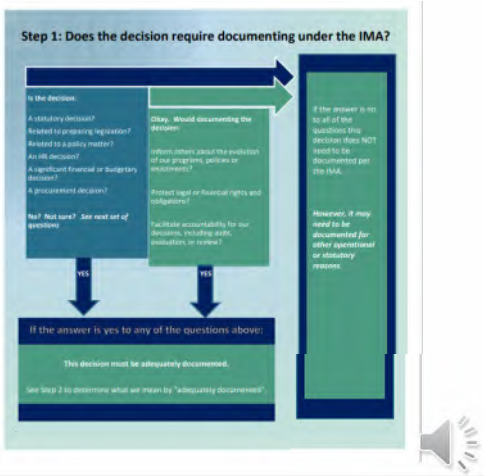
Does the record indicate:

- Who made the decision, and that person's title (position etc.)?
- When the decision was made, and when it takes effect (if appropriate)?
- Who is likely to be affected by the decision (person, group or organization)? Where it is practical, does it indicate how they are affected?
- The basis for or context in which the decision was made? (this includes relevant legal , policy, or factual information)
- Can someone who is not familiar with the circumstances of the decision be reasonably informed about the factors listed above?

If you answered yes to all of those questions - excellent! The record of decision is adequate under the IMA.

If the answer is no to any of those questions, this will require analysis to ensure we are adequately documenting our decisions.

For further clarification, please contact the Records and Information Services team.



13

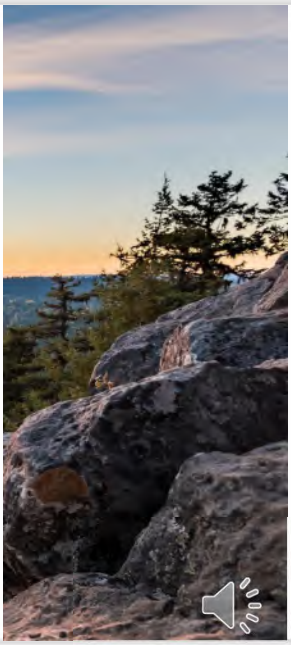
So hopefully this helps you understand the legislative requirement for us to create an adequate record of our key decisions, and ensure they are in a recordkeeping system.
We have created tools to help with this

- A Checklist, which is helpful for list people who want to make a quick assessment, and a
- 2-page process chart, which is a more visual assessment tool.

These are on the Energy Exchange, on the Information Management page, where you will also find an overview. <NEXT SLIDE>

We create records for many reasons. Upholding our accountabilities and legislated requirements regarding managing those records is a best practice.

Thank you for your time.



14

In summary, we create records for many different legislated, policy and operational reasons. Take the time to ensure we uphold our accountabilities regarding documenting and managing our records of decisions.

Thank you for your time.

DOCUMENTING GOVERNMENT DECISIONS (DGD)

The provincial government is assigning a new legislated requirement to government bodies under the *Information Management Act* (IMA): a requirement to **create and maintain adequate records of decisions.**

The Head of each government body will be responsible for ensuring their organization has an appropriate system for documenting decisions in place.

What is an "Adequate" Record of Decision?

A record of decision is adequate if someone who is not familiar with the decision could determine:

- Who made the decision
- When the decision was made (and took effect)
- Who is likely to be affected by the decision
- What is the basis and context in which the decision was made (e.g. relevant legal, policy or factual information)

Not all factors noted above will apply to every decision. For example, some decisions do not affect others. In some cases, an adequate record of a decision may be a note in a file. In others, it may include copies of extensive studies, or a combination of records.

The nature of the decision will determine the amount and type of contextual information necessary. An adequate record might consist of:

- Briefing notes for decision
- Application forms
- Submissions from industry
- Entries into systems/databases
- Emails, letters, etc. containing advice, recommendations or options
- Records of verbal advice
- Legal opinions
- Orders

NOTE: Part of understanding the context for decisions is having clear roles and responsibilities, or frameworks, regarding decision-making. These are often established through job descriptions, training, policies or procedures, and process mapping and documentation.

What Decisions Need to be Documented?

The Commission does not need to create records of every decision made by every employee. We can apply judgement. Typically, we should document decisions that relate to the:

1. Evolution of Commission programs.
2. Protection of the Commission's legal or financial rights or obligations, or those affected by a decision.
3. Facilitation of the Commission's accountability.

Specifically, this may include:

- **Line of business** (operational) decisions
- **Statutory** decisions (e.g. directives, orders, authorizations, permits)
- Decisions related to **preparing legislation** (e.g. analysis, developing a request for legislation and drafting process records)
- Decisions about **policies, programs or initiatives that fulfill the Commission's mandate** (e.g. records supporting the establishment, change or termination of corporate direction)
- Decisions about **Human Resource** (HR) matters
- **Budgeting** and **financial** decisions
- **Procurement** decisions (e.g. records of goods purchasing, contractor services, IT procurement)

NOTE: While there is a records management component to the documenting government decisions requirement, this is really about corporate accountability, transparency and ensuring best practices are in place.

Where Should Records of Decisions be Kept?

The Commission has a variety of recordkeeping systems: program folders on shared drives, databases, hardcopy files, etc.

Records of decision should be kept in a location that ensures their preservation and accessibility (by authorized staff) and appropriate retention in accordance with Commission information schedules.

Tip: See our *What is a Recordkeeping System* guide for ideas on how to manage records of decision.

Step 1: Does the decision require documenting under the IMA?

First, ask whether the decision is:

- ☐ a statutory decision?
- ☐ related to preparing legislation?
- ☐ related to a matter of policy?
- ☐ an HR decision?
- ☐ a significant financial or budgetary decision?
- ☐ a procurement decision?

If the answer is **yes** to any of those questions, the decision must be adequately documented per the IMA.

If the answer is **no**, or you are not sure, ask yourself if documenting the decision would:

- ☐ inform others about the evolution of our programs, policies or enactments?
- ☐ protect legal or financial rights and obligations?
- ☐ facilitate accountability for our decisions, including audit, evaluation or review?

If the answer is **yes** to any of those questions, the decision must be adequately documented per the IMA.

If the answer is **no**, the decision does not need to be documented per the IMA. However, it may need to be documented for other operational or statutory reasons.

Step 2: Is the record of a decision adequate under the IMA?

There are a series of questions you can ask to determine if the record is adequate.

Does the record indicate:

- ☐ Who made the decision, and that person's title (position etc.)?
- ☐ When the decision was made, and when it takes effect (if appropriate)?
- ☐ Who is likely to be affected by the decision (person, group or organization)? Where it is practical, does it indicate how they are affected?
- ☐ The basis for or context in which the decision was made? (this includes relevant legal, policy, or factual information)
- ☐ Can someone who is not familiar with the circumstances of the decision be reasonably informed about the factors listed above?

If you answered **yes** to all of those questions - excellent! The record of decision is adequate under the IMA.

If the answer is **no** to any of those questions, this will require analysis to ensure we are adequately documenting our decisions.

For further clarification, please contact the Records and Information Services team.

Step 1: Does the decision require documenting under the IMA?

Is the decision:

A statutory decision?

Related to preparing legislation?

Related to a policy matter?

An HR decision?

A significant financial or budgetary decision?

A procurement decision?

No? Not sure? ***See next set of questions***

YES

Okay. Would documenting the decision:

Inform others about the evolution of our programs, policies or enactments?

Protect legal or financial rights and obligations?

Facilitate accountability for our decisions, including audit, evaluation, or review?

YES

If the answer is yes to any of the questions above:

This decision must be adequately documented.

See Step 2 to determine what we mean by "adequately documented".

If the answer is no to all of the questions this decision does NOT need to be documented per the IMA.

However, it may need to be documented for other operational or statutory reasons.

Step 2: Is the record of the decision adequate under the *IMA*?

1

Does the record indicate:

Who made the decision, and that person's title (position etc.)?

When the decision was made, and when it takes effect (if appropriate)?

Yes? See 2.

NO

2

Does the record indicate:

Who is likely to be affected by the decision (person/group, or organizations) ?

Where it is practical, how they are affected?

Yes? See 3.

NO

3

Does the record indicate:

The basis for, or context in which the decision was made?

(this includes relevant legal, policy or factual information)

Yes? See next.

NO

If the answer is **no** to any of these questions, this may require some analysis to ensure you are adequately documenting decisions.

Our overarching question:

Can someone who is not familiar with the circumstances of the decision be reasonably informed about the factors previously listed?

Did you answer yes to all of those questions?

GREAT!

The record of decision is adequate under the IMA.

Documenting Commission Decisions under the *Information Management Act (IMA)*
Self-Assessment Gap Inventory

Date:

Team / Program Area

Prepared by:

This form is an optional tool for assessing our compliance with the legal obligation to document key decisions of the Commission.
If you have identified an area for improvement, you may use this form to record the next steps towards compliance.

Decision Description	Decision must be documented because (see STEP 1 flowchart)	Record of decision is not adequate because (see STEP 2 flowchart)	The system for where documentation is kept must be improved because	Next Steps
***Example**:* *Corporate Policy Update*	*Documenting the decision would inform about the evolution of XYZ policy change.*	*Records do not indicate who made the decision (position, branch, etc.)*	*Not applicable*	*Adjust template to reflect position title of decision maker*

Documenting Commission Decisions under the *Information Management Act (IMA)*
Self-Assessment Gap Analysis Template

Decision Description	Decision must be documented because (see STEP 1 flowchart)	Record of decision is not adequate because (see STEP 2 flowchart)	The system for where documentation is kept must be improved because	Next Steps

Documenting Commission Decisions

AN OVERVIEW

Records and Information Services
BC OIL AND GAS COMMISSION

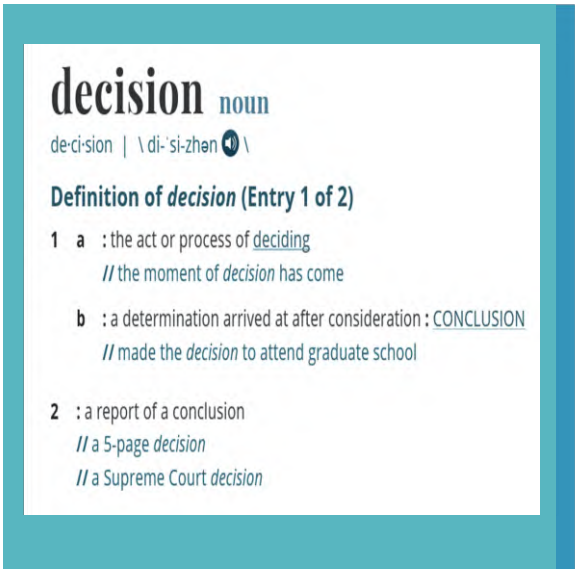
DOCUMENTING COMMISSION DECISIONS

TABLE OF CONTENTS

Why are we talking about this? 2
What do we mean by a “key decision”? 3
What is an “adequate” record of decision? 4
Putting it into practice: examples 5
Summary 6

Why are we talking about this?

On March 31, 2019, the provincial government adopted a new legislated requirement under the *Information Management Act* (IMA): a requirement to ensure we are adequately **documenting government decisions.**



While this has long been considered a best practice, embedding this requirement in legislation makes it a corporate accountability and legislative compliance matter.

This is a good thing! Ensuring we keep a record of our key decisions:

- supports openness and transparency
- facilitates effective decision making
- preserves our corporate memory
- helps us do our jobs more effectively

It also supports accurate reporting of decisions to stakeholders, and provides context for our actions as a government and regulatory body.

We make decisions every day

As Commission employees, we make decisions every day – some minor, some significant. The decisions you make depend on the services you provide and the work that you do. For example, in the Commission, we hire people, we assess industry applications, we create external audit programs, and we develop systems that support our workflow.

The focus here is on whether we are adequately documenting our **key decisions**. We do not need to create records of every decision. We can apply our professional judgement to identify which decisions should be documented, and determine how best to prepare adequate records of those decisions. It is about being accountable and transparent.

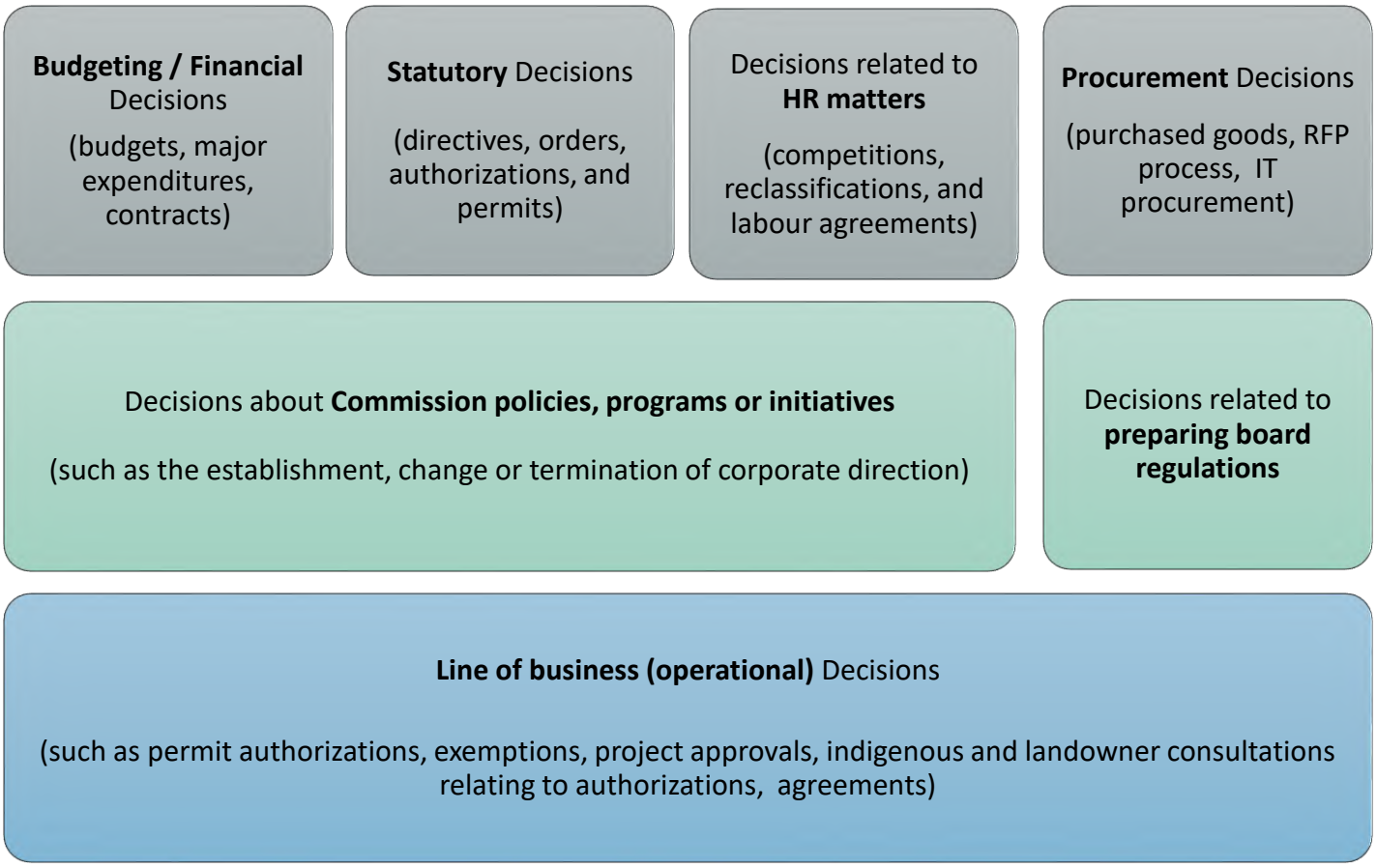
See next page to define "key decisions"…

What do we mean by a key decision?

Typically, a key decision is one that supports one or more of the following:

1. The evolution of Commission programs, policies or enactments
2. The protection of legal or financial rights or obligations of the Commission, or of those affected by a decision
3. The Commission's accountability for its decisions, including through internal or external evaluation, audit or review

EXAMPLES OF KEY DECISIONS THAT MAY REQUIRE ADEQUATE DOCUMENTATION



Documenting decisions made by Senior Executive will often meet the above purposes.

What is an "Adequate" record of decision?

A record of decision is adequate if someone who is not familiar with the decision could determine:

- **Who** made the decision, and under what authority
- **When** the decision was made (and took effect)
- **Who** is likely to be affected by the decision
- **What** is the basis for the decision, and context in which the decision was made (e.g. relevant legal, policy or factual information)

Not all factors noted above will apply to every decision.

Adequate records take different forms

What is considered adequate can vary greatly, depending on the decision. In some cases, an adequate record of a decision may be a note in a file, or a one-page form. Other decisions may be supported by thousands of pages of analysis and advice. The record of decision should be proportionate to the nature, impact and importance of the decision.

Adequate records include context

An adequate record is more than just the "decision" itself. We want to be sure that the context for the decision is part of the record. Remember, our goal is for a person unrelated to the original decision-making process to understand who made it, why it was made, and what information it was based on.

The record of decision should be proportionate to the nature, impact and importance of the decision.

Examples of what an adequate record might include:

- Briefing notes for decision
- Application forms
- Submissions from industry
- Supporting analysis, or technical reports
- Entries into a system or database (such as AMS)
- Emails, letters, etc. that have advice, recommendations or options
- Records of verbal advice (such as notes from a phone call)
- Legal opinions
- Policies and procedures
- Orders
- An email which holds the entire "thread" of a conversation leading to a decision
- Investigation reports

So… what does this look like? Here are some Commission examples:

Putting this into practice #1: Compliance and Enforcement

There is a reported incident on a well, to which we respond. An order is issued to address immediate concerns, and we start a compliance investigation to determine cause. When the investigation is complete, the investigator creates a contravention report, outlining the findings. A decision is made and we issue an administrative penalty. The administrative finding is ***a key decision*** *that requires adequate documentation.* ***The contravention report, the order, supporting documentation gathered to support the decision, and the administrative finding document form the record of decision****.*

This is an example where multiple records support the decision.

Putting this into practice #2: Permit approval process

An operator submits a permit application online, which is processed through AMS. The permit requires landowner consultation, indigenous consultation, and technical review. Each staff member involved in those areas of review document their results in AMS, and the Decision Maker reviews all external and internally submitted information before deciding whether to issue the permit. ***The application information, consultation notes, approved technical specifications, and the permit in AMS are all part of the record of decision.*** *Our governing legislation, Permit Operations and Administration Manual, and documents that outline the authority of the Decision Maker also provide context to the decision.*

This is an example where the record of decision resides in an operational system, where many people contribute to the decision, and where policy and legislation provide context.

Putting this into practice #3: Procurement / RFP process

The Records and Information Services (RIS) team has approval to hire a consultant to help implement the newly approved ORCS on the shared drives. They put together an RFP with their requirements, and work with Finance who vets the RFP, posts it, and manages the RFP process. When the RFP closes, Finance sends the submissions to RIS, who performs a detailed review with an evaluation team, and selects the successful proponent. RIS sends the evaluation notes and decision to Finance, because Finance holds the official RFP file. ***The posted RFP document, the received submissions, the evaluation criteria and selection notes form the record of decision.***

This is an example where two program areas are part of a process, but one holds the official record.

Putting this into practice #4: Decisions made by Senior Executive

The Orphan well program has come up with two options to resolve an arising issue. They outline the options in a Briefing Note, and attach supplemental information to it. Senior Executive discuss the issue, decide on the preferred solution and sign it off. ***The signed briefing note, with the supplemental information, forms the record of decision.***

Alternatively, an email with the two options is sent to their VP, and an email conversation ensues. The VP approves one of the options in the final email of the "thread". ***That final email, containing the back and forth conversation and all attachments, forms the record of decision****.*

This is an example where Executive records document the decision, and where emails include key decisions.

DGD does not change or affect our recordkeeping systems. We continue to keep our records in our shared drives and systems, and our records retention schedules (ARCS and ORCS) still apply according to the function the decision supports.

Summary

The Documenting Government Decisions legislative requirement makes sure we know the "who, what, when and why's" of our key decisions. When you are part of an important Commission decision, consider whether the record is adequate by asking **"Could a person unrelated to the decision-making process understand this decision?"**

We invite you to check out our optional Self-Assessment Guide, which includes decision diagrams, and a template for documenting the areas where we may have room for improvement. The self-assessment exercise will help us identify any gaps, and define those areas where we can improve.

While we are confident that the Commission is already applying this best practice in most areas, an informal examination of our decision-making practices will ensure we are consistently excellent.

We hope this helps you understand the requirement to document Commission decisions.
For further clarification, please contact the Records and Information Services team.

Documenting Commission Decisions

SELF-ASSESSMENT EXERCISE: FINDING THE GAPS

Records and Information Services
BC OIL AND GAS COMMISSION

DOCUMENTING COMMISSION DECISIONS: SELF-ASSESSMENT

TABLE OF CONTENTS

What do we need to do? 2
Decision Diagram, Step 1: determining which decisions require documentation 3
Decision Diagram, Step 2: determining if the decision record is adequate 4
Checklist and Self-Assessment Gap Analysis Template 5

Request BCER2024-010 - Page 56 of 234

The provincial government has adopted a legislated requirement under the *Information Management Act* (IMA) to **document government decisions.** This is a flexible framework to ensure we are adequately documenting our important decisions.

Please refer to our *Documenting Commission Decisions Overview* for a full understanding of this initiative.

What do we need to do?

We need to look at our practices and ensure we have adequate documentation of our key decisions.

This will not be difficult! On the following pages, you will find some helpful documents for assessing our compliance with this requirement:

- ✓ A diagram to help assess whether the decisions you make require "adequate documentation"
- ✓ A diagram to determine "adequacy" (we are aiming for adequate, not perfect)
- ✓ A simple yes/no checklist to use when working through an evaluation
- ✓ An optional template for recording process gaps

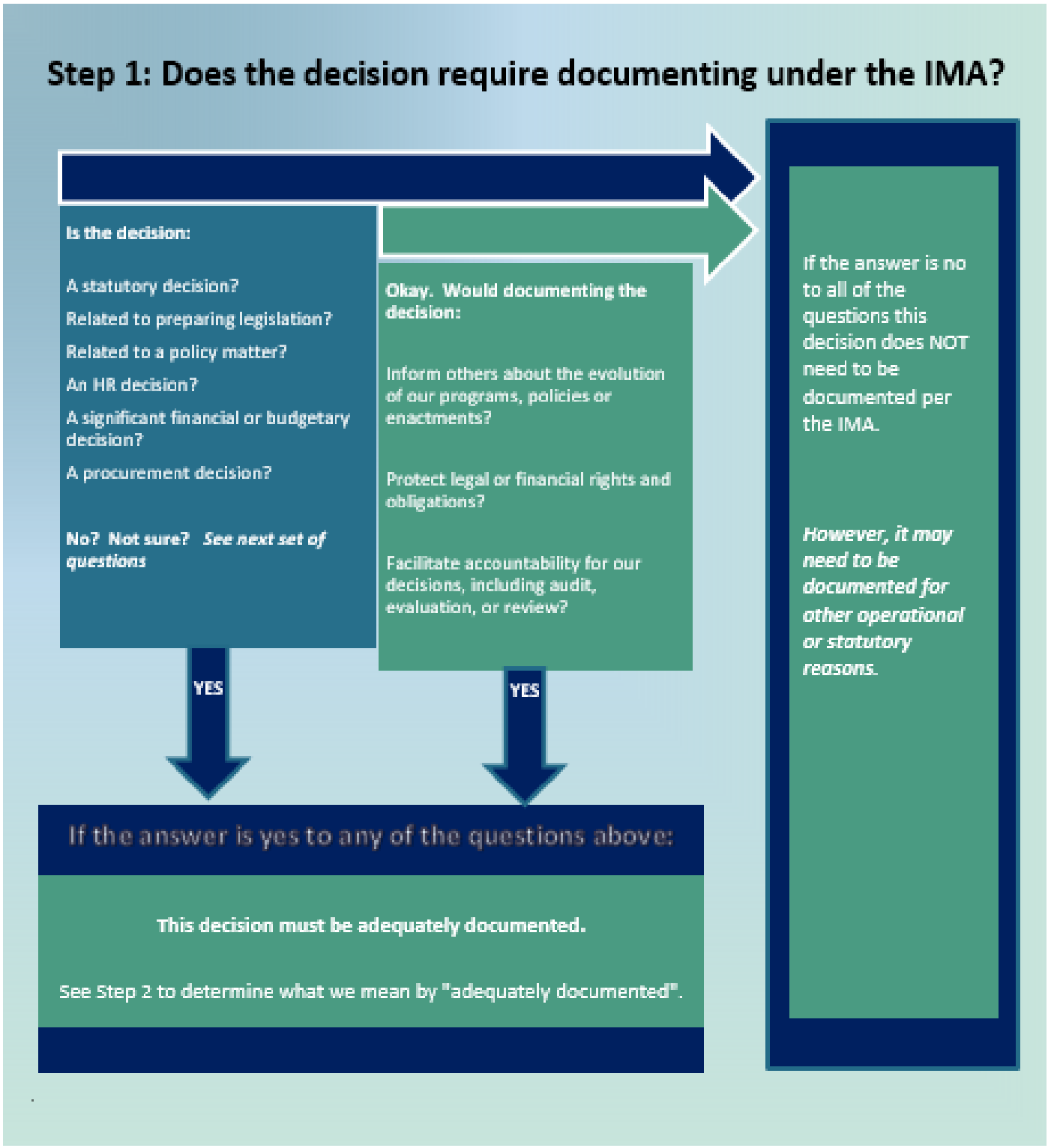
It only takes a few steps:

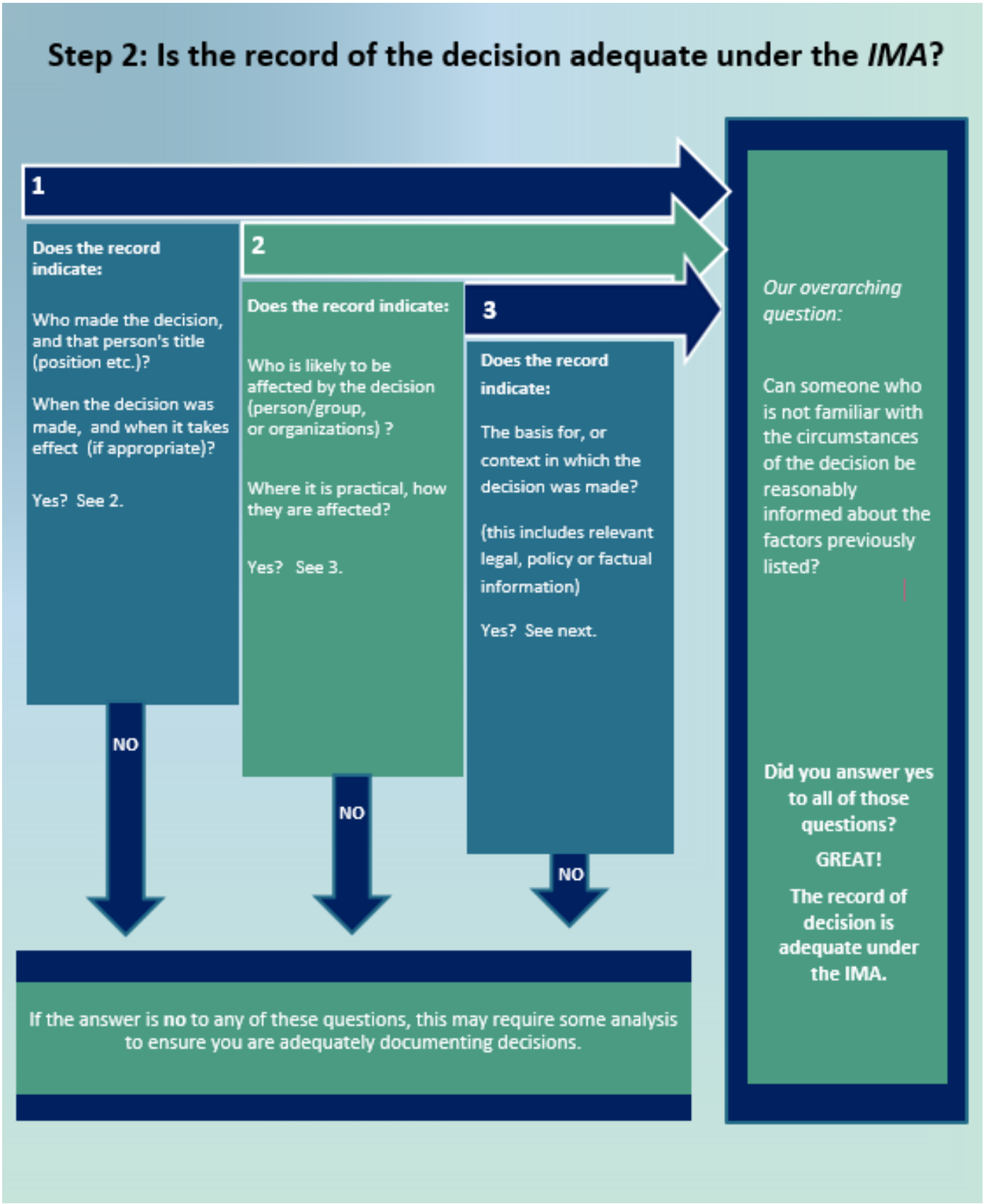
1. Look at your mandated responsibilities to help identify the decisions that support them
2. Determine which of those decisions require an evaluation to ensure we have an adequate record
3. Review how those decisions are documented to assess our state of compliance
4. If you identify any gaps, you will need to take action to improve your processes

If you would like help in determining the best solution to a gap, please contact us at Records and Information Services (RIS) and we will be happy to work with you!

See the next page for assessment diagrams

Request BCER2024-010 - Page 57 of 234


Step 1: Does the decision require documenting under the IMA?
Is the decision:
A statutory decision?
Related to preparing legislation?
Related to a policy matter?
An HR decision?
A significant financial or budgetary decision?
A procurement decision?
No? Not sure? See next set of questions
YES
Okay. Would documenting the decision:
Inform others about the evolution of our programs, policies or enactments?
Protect legal or financial rights and obligations?
Facilitate accountability for our decisions, including audit, evaluation, or review?
YES
If the answer is no to all of the questions this decision does NOT need to be documented per the IMA.
However, it may need to be documented for other operational or statutory reasons.
If the answer is yes to any of the questions above:
This decision must be adequately documented.
See Step 2 to determine what we mean by "adequately documented".

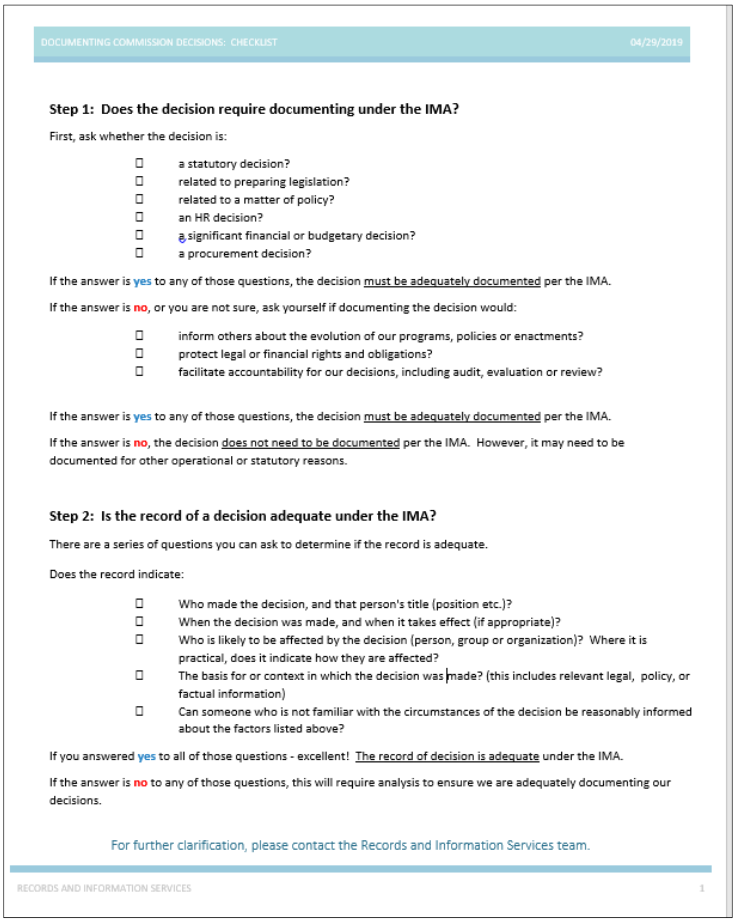

Step 2: Is the record of the decision adequate under the *IMA*?
1
Does the record indicate:
Who made the decision, and that person's title (position etc.)?
When the decision was made, and when it takes effect (if appropriate)?
Yes? See 2.
NO
2
Does the record indicate:
Who is likely to be affected by the decision (person/group, or organizations) ?
Where it is practical, how they are affected?
Yes? See 3.
NO
3
Does the record indicate:
The basis for, or context in which the decision was made?
(this includes relevant legal, policy or factual information)
Yes? See next.
NO
If the answer is **no** to any of these questions, this may require some analysis to ensure you are adequately documenting decisions.
Our overarching question:
Can someone who is not familiar with the circumstances of the decision be reasonably informed about the factors previously listed?
Did you answer yes to all of those questions?
GREAT!
The record of decision is adequate under the IMA.

A consideration before you begin:

Part of understanding the context for decisions is having clear roles and responsibilities, or frameworks, regarding decision-making. These may established through job descriptions, training, policies or procedures, and process maps. Consider them when determining adequacy.

Tools to help with this process (found on MyOGC)

This **yes/no checklist** may help when evaluating the adequacy of your recorded decisions.



DOCUMENTING COMMISSION DECISIONS: CHECKLIST 04/29/2019

Step 1: Does the decision require documenting under the IMA?

First, ask whether the decision is:

- ☐ a statutory decision?
- ☐ related to preparing legislation?
- ☐ related to a matter of policy?
- ☐ an HR decision?
- ☐ a significant financial or budgetary decision?
- ☐ a procurement decision?

If the answer is yes to any of those questions, the decision must be adequately documented per the IMA.

If the answer is no, or you are not sure, ask yourself if documenting the decision would:

- ☐ inform others about the evolution of our programs, policies or enactments?
- ☐ protect legal or financial rights and obligations?
- ☐ facilitate accountability for our decisions, including audit, evaluation or review?

If the answer is yes to any of those questions, the decision must be adequately documented per the IMA.

If the answer is no, the decision does not need to be documented per the IMA. However, it may need to be documented for other operational or statutory reasons.

Step 2: Is the record of a decision adequate under the IMA?

There are a series of questions you can ask to determine if the record is adequate.

Does the record indicate:

- ☐ Who made the decision, and that person's title (position etc.)?
- ☐ When the decision was made, and when it takes effect (if appropriate)?
- ☐ Who is likely to be affected by the decision (person, group or organization)? Where it is practical, does it indicate how they are affected?
- ☐ The basis for or context in which the decision was made? (this includes relevant legal, policy, or factual information)
- ☐ Can someone who is not familiar with the circumstances of the decision be reasonably informed about the factors listed above?

If you answered yes to all of those questions - excellent! The record of decision is adequate under the IMA.

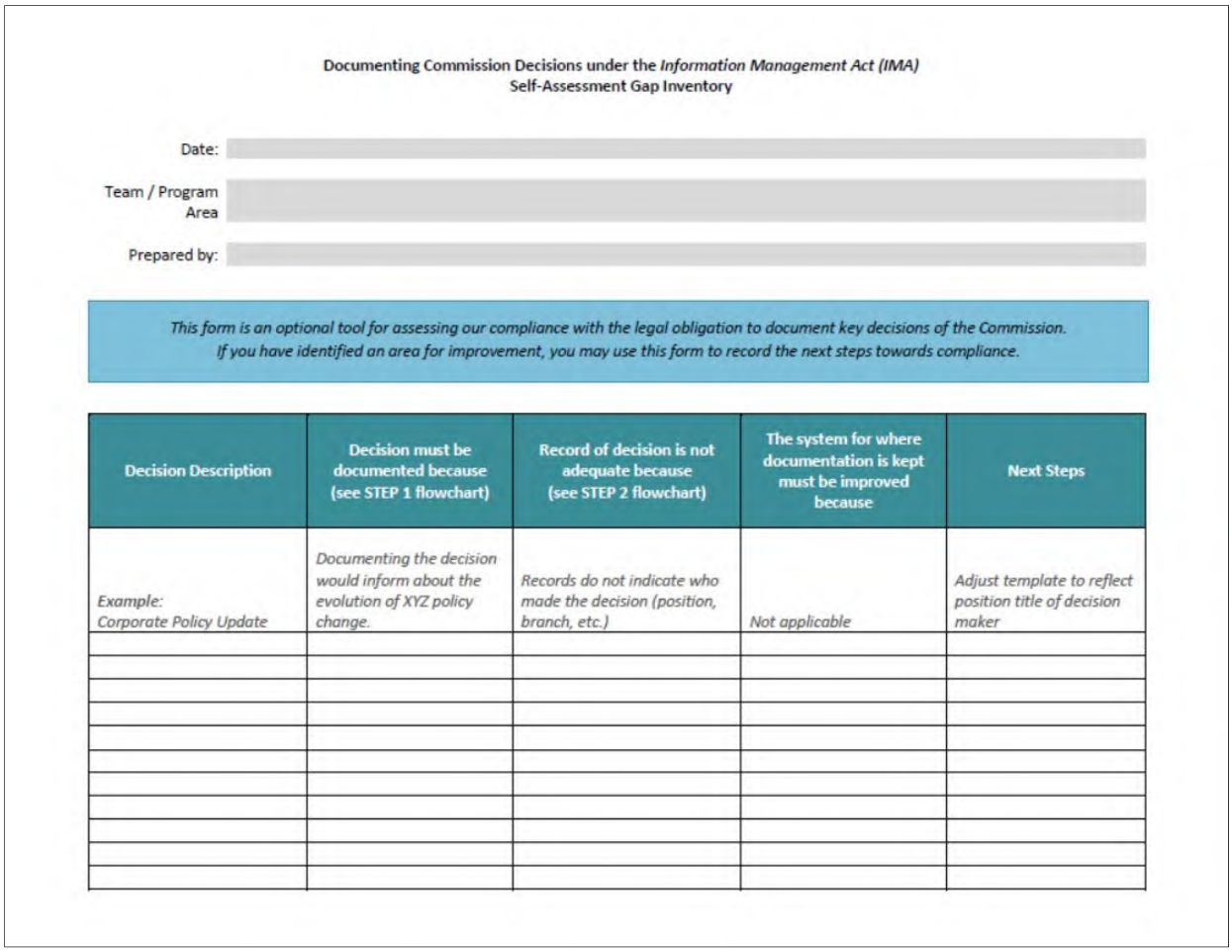
If the answer is no to any of those questions, this will require analysis to ensure we are adequately documenting our decisions.

For further clarification, please contact the Records and Information Services team.

RECORDS AND INFORMATION SERVICES 1

Self-Assessment Gap Inventory

You may use this optional template to document any gaps in your processes.



Documenting Commission Decisions under the *Information Management Act (IMA)*
Self-Assessment Gap Inventory

Date:

Team / Program Area

Prepared by:

This form is an optional tool for assessing our compliance with the legal obligation to document key decisions of the Commission. If you have identified an area for improvement, you may use this form to record the next steps towards compliance.

Decision Description	Decision must be documented because (see STEP 1 flowchart)	Record of decision is not adequate because (see STEP 2 flowchart)	The system for where documentation is kept must be improved because	Next Steps
Example: Corporate Policy Update	*Documenting the decision would inform about the evolution of XYZ policy change.*	*Records do not indicate who made the decision (position, branch, etc.)*	*Not applicable*	*Adjust template to reflect position title of decision maker*

Finally, what to do with those documented decisions

A record of decision may reside in more than one place, since record keeping systems in the Commission take a few shapes. We use business systems to document decisions, such as permit approvals in AMS, or inspection notes in Kermit. We use shared drives to manage our electronic documents. In some areas, we still use paper files. Any of those options are appropriate record keeping systems, as long as you use them consistently.

This requirement does not change how you manage your records, or what ARCS/ORCS number should apply to them; it just requires you to be sure you have an adequate record of important decisions.

We hope this helps you assess your compliance with the requirement to document Commission decisions. For further clarification, please contact the Records and Information Services team.

Request for Proposals

All enquiries related to this Request for Proposals, including any requests for information and clarification, are to be submitted by **December 4, 2020** and directed, in writing, to **Bradley.Weaver@bcogc.ca,** who will respond if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Commission's option.

RFP #21221015

Defining System Requirements for Electronic Document and Records Management

Closing Time: Proposal must be received electronically **before 2:00 PM** Pacific Time on: **December 18, 2020**

Organization Overview

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for overseeing oil and gas operations in British Columbia. Regulatory responsibility is delegated to the Commission through the *Oil and Gas* Activities *Act* and includes specified enactments under the *Forest Act, Heritage Conservation Act, Land Act, Environmental Management Act*, and *Water Act*. The operating costs of the Commission are funded through industry fees and levies on a cost recovery basis.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected by ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

The regulatory responsibility of the Commission extends from the exploration and development phases of oil and gas activities through to facilities operation, and ultimately decommissioning of industry projects. It is charged with balancing a broad range of environmental, economic and social considerations.

1. Summary of the Requirement

The BC Oil and Gas Commission (Commission) is seeking interested parties to undertake a detailed assessment of requirements for effectively managing the end-to-end life cycle of its official records in accordance with provincial legislation, policies and standards for government record-keeping.

The *Ministry of Management Services' 2001 Enterprise Document and Records Management System RFP* (see Appendices) should be referenced as a requirements benchmark, where applicable to the Commission's specific business needs and scale.

This work will provide the Commission with a clearly defined baseline for a "total" records management solution available to all employees.

2. Anticipated Schedule

The following table outlines the anticipated schedule for this RFP. All times identified in the table are in Pacific Time.

Event	Anticipated Date
Enquiries deadline	December 4, 2020
Request closing time	December 18, 2020
Interviews as required	January 4-8, 2021
Preferred Proponent selected by	January 11, 2021
Commencement of work	January 15, 2021

3. Commission Situation/Overview

The Commission is the provincial regulatory agency for permitting and overseeing oil and gas activities, from exploration and development through to operations and ultimately decommissioning of oil and gas industry projects under British Columbia jurisdiction. The Commission's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2020/21 - 2022/23 Service Plan available on the Commission's website at www.bcogc.ca.

3.1 Commission Responsibility

Oil and Gas Activities Act (OGAA):

The purposes of the Commission, outlined in Section 4 of the Oil and Gas Activities Act, are briefly summarized as follows:

(a) to regulate oil and gas activities in British Columbia in a manner that
    (i) provides for the sound development of the oil and gas sector, by fostering a healthy environment, a sound economy and social well-being,
    (ii) conserves petroleum and natural gas resources,
    (iii) ensures safe and efficient practices, and
    (iv) assists owners of petroleum and natural gas resources to participate equitably in the production of shared pools of petroleum and natural gas;
(b) to provide for effective and efficient processes for the review of applications for permits and to ensure that applications that are approved are in the public interest having regard to environmental, economic and social effects;
(c) to encourage the participation of First Nations and aboriginal peoples in processes affecting them;
(d) to participate in planning processes;
(e) to undertake programs of education and communication in order to advance safe and efficient practices and the other purposes of the commission.

Information Management Act (IMA):

The Commission is subject to the provisions of the Information Management Act (IMA), government's primary information management law. This legislation was brought into force in 2016 to modernize government practices. Compliance with the IMA requires public bodies to transition from hard copy to digital storage and information management, and implement appropriate systems to support this.

A legislative amendment in 2019 added a requirement for the head of a government body to ensure that an appropriate system is in place for creating and maintaining government information that is an adequate record of that government body's decisions.

Section 19 of the IMA defines the responsibility of the head, as follows:

Responsibility of head of government body

19 (1) The head of a government body is responsible for ensuring that an appropriate system is in place within the government body for managing and securing government information.

(1.1) Without limiting subsection (1), the head of a government body is responsible for ensuring that an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines issued under section 6 (1) *[directives and guidelines]*, government information that is an adequate record of that government body's decisions.

(2) The head of a government body must take reasonable steps to ensure that the government body
    (a) complies with directives issued under section 6 (1), and
    (b) is guided by guidelines issued under that section.

(3) [Repealed 2017-7-5.]

(4) The head of a government body must take reasonable steps to ensure that the government body complies with the following:
    (a) [Not in force.]
    (b) section 10 *[when information schedule applies]*;
    (c) section 13 *[information must be digitized before archiving]*.

(5) Despite subsection (4) (b), the head of a government body must ensure that no government information held by the government body is disposed of, except in accordance with an information schedule or an approval by the chief records officer under section 11 (1) (b) *[when no information schedule applies]*.

3.2 Current Situation

The BC Oil and Gas Commission (Commission) has a complex array of information with long term value to the province, and a continuously evolving business and regulatory environment. As a government body, the Commission is required to manage its records using the government standard for classification, retention and disposition, including the *Administrative Records Classification System* (ARCS), the Commission's *Operational Records Classification System* (ORCS) and other approved records schedules. An integrated software solution has been recognized as necessary for meeting this responsibility and effectively managing Commission information, regardless of media, from creation to final disposition.

To support this, the Records and Information Services and Information Systems and Technology branches initiated a two phased-approach to achieving a state of readiness. The first phase was initiated in 2017/18 and included modernization of the Commission's outdated Operational Records Classification System (ORCS), with the objective of:

- Achieving media neutrality (to ensure official records can exist in any format);
- Addressing functional gaps within the classification system (to ensure all records are covered); and
- Reviewing record retention periods for appropriateness (to ensure records are being retained long enough to meet business and legal requirements).

The second phase commenced in fiscal 2019/20, and includes the classification of electronic program records on shared drives in accordance with the Commission's amended and approved ORCS, ARCS, and other applicable schedules. Phase 2 is ongoing and recognized as a long term initiative.

The Commission is migrating to Microsoft Office 365 (M365) and Azure for enterprise usage. A subsequent gap analysis project is anticipated, which will evaluate the commission's records management and user requirements against the functionality M365 offers.

3.3 Budget/Schedule

Funding to support this project in fiscal year 2020/2021 is $30,000. Proponents are encouraged to provide their best, realistic estimate for the work that they propose to meet the Commission's requirements. The Commission welcomes innovative proposals that reduce costs or duration, or that provide added value. Proponents are invited to describe and provide separate costing for the two Phases.

Proposed timelines must target delivery of the requirements assessment by the end of fiscal year 2020/2021. Subsequent phases may be awarded at the Commission's discretion based on the success of the initial project and available funding.

3.1 Scope of Services

The successful Proponent who enters into a written contract with the Commission is expected to provide the following services:

1. Assess and clearly define Commission records management requirements to address business needs.
2. Project schedule, communications and reporting – proponent resources must be able to define project timelines, support meetings and/or reporting at the discretion of the Commission including regular status reports to inform on progress, risks, issues, spend to date, etc.
3. Project closure – proponent resources to be available to participate in project close out activities as required.

All deliverables will require the approval of the Commission before being accepted.

The Commission's Records and Information Services Branch provides cross-organization guidance on corporate records management requirements and will serve as the primary project contact. The Branch Director, and Specialist, EDRMS & Information Management Solutions will act as project managers and work directly with the proponent as agreed to by both parties. The Director of Information Systems Branch will be involved to provide necessary oversight, system information and help facilitate contract deliverables.

3.2 Scope of Work

3.2.1 Identification of Business Needs

1. The project will involve engagement with the Commission's Records and Information Services Branch to identify business and user requirements as they relate to established information management best practices and compliance requirements.
2. Proponent will base the assessment on:
    a. BC Government records and information management policy and standards, and compliance requirements;
    b. provincial electronic document record management system requirements (Appendices E and F);
    c. an understanding of the Commission's current hybrid records and information management environment and associated processes;
    d. an understanding of the Commission's records classification and retention requirements;
    e. an understanding of the Commission's operations, objectives and business needs; and
    f. with an awareness of the Commission's current system and technological environment.

3.3 Deliverables

Project deliverables will include:

1. A records management requirements document (SRS) establishing specific criteria for the Commission, which will serve as the framework for a gap analysis against functionality implemented with Microsoft 365. A template will be provided.
2. A project schedule.
3. Status reports as required. A template will be provided.
4. Monthly invoicing.

3.4 Format Requirements

The following format, sequence, and instructions must be followed in order to provide consistency in Proponent response and ensure each proposal receives full consideration. With all pages consecutively numbered, the proposals should contain the following parts:

a) Table of contents with page numbers.

b) One page executive summary.

c) The body of the proposal in accordance with the content requirements.

3.5 Content Requirements

Responses should be succinct and should focus on specific products and services being proposed – please be considerate of the time it will take to review the submission.

In order to expedite a fair and unbiased proposal review process, the Commission's preference is for all proposals to use the following outline:

a) Project Approach (description the proposed approach, based on the scope described in section 4.1)

b) Costs/Schedule (including hourly rates, overall timelines and total cost) provided in Canadian dollars (CAD).

c) Overall timeline

d) Budget breakdown

e) One example of **relevant** previous work (optional)

f) Resumes (max half page each)

4. Evaluation of Proponent Response

The evaluation of responses will be conducted by a team consisting of employees and/or contractors of the Commission. All members of the team will be bound by the same standards of confidentiality.

This section details all of the mandatory and desirable criteria against which proposals will be evaluated. Proponents should ensure that they fully respond to all criteria in order to receive full consideration during the evaluation.

The lowest price or any Proposal will not necessarily be accepted. The Commission reserves the right to refuse any proposed based on quality, service, price, reputation, experience and other criteria.

The Preferred Proponent will be the Proponent scoring the most points after evaluation. The evaluation process will consist of the following stages:

- Stage One – Mandatory Criteria
- Stage Two – Desirable Criteria
- Stage Three – Informational Interviews (optional and not scored)

4.1 Mandatory Criteria

Proposals not clearly demonstrating that they meet the following mandatory criteria will be excluded from further consideration during the evaluation process:

- **The Proposal must be sent and received before the designated closing date and time.**
- **The Proposal must be in English and submitted electronically to** https://procurement.bcogc.ca/
- **The Proponent must confirm that any personal information received, collected or held over the course of the review will be stored and used only in Canada.**
- **The Proposal must contain an independence and objectivity statement confirming the Proponent is free of any actual or perceived conflict of interest and free of bias with respect to the Commission, its officers and employees.**

Failure to meet all mandatory criteria above will disqualify the Proponent's Proposal from further review.

4.2 Desirable Criteria

The Commission seeks to enter into an agreement with the Proponent who, in the opinion of the Commission, has the resources, knowledge and competence to provide the greatest value. Proposals meeting all of the mandatory criteria will be further assessed against desirable criteria.

Desirable Criteria	Weight
Proponent's Qualifications and Relevant Experience	30%
Suitability of Proposed Approach • Proposal demonstrates Proponent's understanding of government's records management policy and compliance framework. • Proposal provides a clearly defined plan to address project requirements.	45%
Pricing • Total price, hourly rate	25%

4.3 Informational Interviews

The top ranking (to a maximum of three) Proponents may be asked to attend an interview with the evaluation team. During the interview, the evaluation committee may clarify and/or verify statements made in the written Response.

The requirement for interviews is optional. The Commission reserves the right to complete the evaluation process without Proponent interviews.

5. Appendices

5.1 BC Government EDRMS RFP, Appendix E: High Level Requirements (Records Management)
5.2 BC Government EDRMS RFP, Appendix F: Desirable System Requirements

The entire BC Government RFP is available at: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-management/edrms/edmsrfp.pdf

Appendix E High Level Requirements (Records Management)

File: *ARCS* 420-25/RMBR
Date: June 20, 2001

BC GOVERNMENT
RECORDS MANAGEMENT BUSINESS REQUIREMENTS

Prepared by the Records Management Business Requirements Working Group:
(ministry names reflect pre-reorganisation structure)

Drew Smyth (Chair), Ministry Records Officer, Ministry of Environment, Lands and Parks
Ellinore Barker, Corporate Records Officer, Information, Science and Technology Agency (ISTA)
Peter Freeman, Manager, Corporate Information Services Branch, Information Technology Services Division, ISTA
Heather Mackay, Electronic Records Analyst, BC Archives, ISTA
Mary McIntosh, Ministry Records Officer, Ministry of Health
Jaye Pelton, Business Analyst, BC Archives, ISTA
Beth Pitblado, Ministry Records Officer, Ministry of Transportation and Highways and Records Officer responsible for BC Fisheries

BC Government Records Management Business Requirements

Table of Contents

E1 INTRODUCTION 39

E1.1 WHAT IS A RECORD? 39
E1.2 DOCUMENT VS. RECORD 39
E1.3 WHAT IS RECORDS MANAGEMENT? 40
E1.5 STRUCTURE OF THIS DOCUMENT 40

E2 BUSINESS REQUIREMENTS – LOCATION MANAGEMENT 42

E2.1 RECORD CREATION OR RECEIPT 43
E2.2 IDENTIFYING AND DOCUMENTING RECORDS 43
E2.3 PROFILE INFORMATION (METADATA) 43
E2.4 RECORD MAINTENANCE 44
E2.5 SEARCHING FOR AND RETRIEVING RECORDS 44
E2.6 ACCESS SECURITY 44
E2.7 TRANSFERRING RECORDS TO ANOTHER LOCATION 45

E3 BUSINESS REQUIREMENTS – PRESERVATION MANAGEMENT 45

E3.1 PHYSICAL PRESERVATION OF RECORDS 45
E3.2 INTELLECTUAL PRESERVATION OF RECORDS 45

E4 BUSINESS REQUIREMENTS – SCHEDULING MANAGEMENT 46

E4.1 SCHEDULING MANAGEMENT – ACTIVE RECORDS 46
E4.1.1 Records Classification 46
E4.1.2 Active Status 46
E4.1.3 End of Active Status 47
E4.2 SCHEDULING MANAGEMENT – SEMI-ACTIVE RECORDS 47
E4.2.1 Applying Semi-active Retention Schedules 47
E4.2.2 End of Semi-active Status 48
E4.3 SCHEDULING MANAGEMENT – INACTIVE RECORDS 48
E4.3.1 Applying Final Disposition to Inactive Records 48

BC GOVERNMENT RECORDS MANAGEMENT BUSINESS REQUIREMENTS

E1 INTRODUCTION

The *BC Government Records Management Business Requirements* were developed by a working group of ministry records officers, information technology experts, and central agency analysts. They document the functions and requirements for managing records in the BC government.

Note on terminology: The term "record" is defined broadly in the BC *Interpretation Act* (RSBC 1996, c.238) to include "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise". This definition is used in key information management statutes such as the *Document Disposal Act* (RSBC 1996, c. 99) and the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) to ensure that the provisions of these statutes apply to all forms of recorded information. However, for the purposes of this RFP, the terms document and records are defined more precisely in order to distinguish between the general functions required to create and maintain documents and the more rigorous controls required to capture and manage documents as business records.

E1.1 What is a Record?

A *record* is a document created or received in the course of government business and maintained for action or reference by an agency as evidence of that business.

- Records exist in all media and formats.
- Email messages and attachments are records.
- If a record is copied, the copy is a new and unique record.

E1.2 Document vs. Record

A document is "recorded information which can be treated as a unit" (*ISO s. 3.10*). Any medium that contains information is a document. A document has the status of a record *only* if it is created or received in the course of government business and if it is maintained as evidence of that business. Most documents created or received by government offices are records.

The BC government must manage all documents in compliance with legal and policy requirements. The *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) applies to all documents held by government ministries and agencies, whether they are records or not. In addition, all documents are subject to discovery during litigation, regardless of their record or non-record status.

The *Records Management Business Requirements* focus on records and the processes involved in their management. They do not discuss the requirements relating specifically to document management functions. However, records management and

document management are related and important components of an effective information management infrastructure.

E1.3 What is Records Management?

Records management is the exercise of physical and intellectual control over records to ensure their integrity in support of government accountabilities and actions. Ministries establish physical control by ensuring records are identified, documented, located, retrieved, and protected from loss, physical damage or inappropriate access. Ministries establish intellectual control over their records by ensuring they are classified, retained and disposed of (destroyed or transferred to the legal custody of the BC Archives) in accordance with their values (that is, in accordance with retention and disposition schedules). Retaining records required for operational, administrative, fiscal, audit and legal purposes (while applying the final disposition to the records whose primary values have ceased) reduces on-site and off-site storage expenditures.

E1.4 Records Management Legislative and Policy Structure

Records management in the BC government is governed by legislation and policy and supported by established processes and standards.

- The *Document Disposal Act* (RSBC 1996, c. 99) governs the final disposition of government documents (records and non-records) by specifying the approvals required before they may be destroyed, transferred to the custody of the government archives or alienated from the Crown provincial.
- Responsibilities and accountabilities for managing government records are established by Treasury Board policy through the *General Management Operating Policy (GMOP)* and the *Financial Administration Operating Policy (FAOP)* manuals.
- Classification and scheduling systems, such as the government-wide *Administrative Records Classification System (ARCS)* and program-specific *Operational Records Classification Systems (ORCS).* These systems establish classes of records and determine retention periods and final dispositions that reflect their values.
- The British Columbia Archives (BC Archives) establishes government-wide records management policy through specific guidelines, policies and standards.
- Ministry Records Officers establish ministry policies and procedures in compliance with government-wide policies.

E1.5 Structure of This Document

The *Records Management Business Requirements* cover the physical management of records and the intellectual management of the information contained in records.

Records are subject to actions and processes. They are created, identified, documented, stored, physically transferred, preserved, protected, retained and disposed of. In this document, these actions and processes are addressed in the following three sections: Section 1, “Location Management” relates to the physical management of records in order to access and use them.

Section 2, "Preservation Management" relates to the physical and intellectual maintenance of records in order to preserve the information they contain.
Section 3, "Scheduling Management" addresses how the information contained in records must be managed. Records move through a lifecycle during which they are assigned a status of active, semi-active, or inactive based on a records retention and disposition schedule. This schedule assigns a value to a record that is reflected in its retention period and final disposition. Scheduling management relates to the intellectual management of records in accordance with their values.
In addition, this document contains a glossary of terms (see Definitions, below) that serve to clarify the specific meaning of the terminology used to describe records management business requirements.

Definitions
Terms with specific meaning within the *Business Requirements* document are defined below.

- **Document** is defined as information consigned to a medium. This includes "anything on which there is writing…marks, figures [or] symbols." (*New South Wales, Australia – Evidence Act 1995).* Documents fall into one of two sub-sets:

    1) documents that are also records, or
    2) documents that are not records.

- **File** is defined as the logical entity used to organise and manage records. A file manages a group of records that together provide evidence of a complete transaction or a collection of reference material. A file is not a physical entity. Retention and disposition schedules are applied to records at the file level.
- **File Series** is defined as a collection of files that are managed under one primary-secondary classification and have the same scheduling requirements.
- **Final Disposition** is defined as an action applied to eligible files by destroying them, transferring them to the permanent custody of the government archives, or alienating them from the Crown provincial. Files are eligible for final disposition when their active and semi-active retention periods have elapsed. The records schedule designates the appropriate type of final disposition for a file.
- **Life cycle** is defined as the changes of a file's scheduling status, which moves from active to semi-active to inactive.
- **Location** is defined as the physical location of a file's volume or volumes. The location of a file's volumes does not affect the file's scheduling status.
- **Location management** is defined as managing records so they can be identified, documented, located, viewed, retrieved, copied, and secured from unauthorised access.
- **Preservation management** is defined as managing record media (paper, electronic, micrographic, photographic, cartographic, or any other media) in

order to protect records from loss, damage or degradation. It is also defined as managing recorded information to ensure its authenticity and context as it moves from one media or carrier to another.

- **Record** is defined as "recorded information, in any form…created or received and maintained by an organisation in the transaction of business …and kept as evidence of such activity." (*Australian Standard AS 4390-1996, part 1, clause 4.21*) In the BC government, the record is the indivisible unit for records management processes.
- **Records Classification and Scheduling System** organises files into functional groupings for filing and retrieval (classification) and assigns retention periods and final dispositions to classified records (scheduling). These systems are referred to as integrated classification and scheduling systems, as opposed to systems that provide either classification or scheduling but not both. *ARCS* and *ORCS* are examples of integrated systems.
- **Retention and Disposition Schedule** is the length of time a file is to be retained and the type of final disposition that is applied to it. In an integrated classification and scheduling system (*ARCS/ORCS*), retention and disposition schedules are linked to secondary classification numbers.
- **Retention Period** is the length of time a file is retained, and is determined by the retention and disposition schedule. The file may be disposed only after the active and semi-active retention periods that apply to it have elapsed.
- **Scheduling Management** is defined as managing the retention and disposition of files in accordance with their scheduling requirements.
- **Scheduling Status** is defined as the status of a file in accordance with the retention and disposition schedule that applies to it. A file may have a scheduling status of active, semi-active, or inactive. A file is eligible for final disposition when it is inactive.
- **Volume** is defined as a component of a file. A volume contains records, and may exist in any media or format (e.g. file folder, electronic folder, microfilm roll, map drawer, and so on). Volumes are often referred to as folders, enclosures, directories, supplements, or sub-files. All these terms refer to the components of a file, and are covered by "volume" in these *Requirements*.

E2 BUSINESS REQUIREMENTS – LOCATION MANAGEMENT

Ministries must manage their records regardless of media or format or on-site or off-site storage location. Essential to the management of records is the ability to locate, view, retrieve, copy and control access to records, regardless of their scheduling status.

E2.1 Record Creation or Receipt

Upon receipt or creation, records enter the records management system. Records provide documentary evidence of the ministry's activities in performing the functions for which it is responsible.

- A record may be copied, but the act of copying creates a new and unique record.
- Records should be created or received in media or format appropriate to the way they are used and which meets the requirements of their scheduled retention and disposition. If they are not created or received in appropriate media, they must be converted or migrated to appropriate media or format.

E2.2 Identifying and Documenting Records

Records are documented so they can be identified, retrieved and managed. Records in all media and formats must be documented.

- Records must be classified in accordance with an established classification system.
- Ministries must create indexes, file lists, or other finding aids documenting the attributes of all files and their physical components (volumes) to ensure they can be retrieved and the ministry's record holdings are documented.
- Classification and indexing systems must establish and use controlled language.
- All the volumes relating to a file must be documented.
- Documentation may be amended or corrected.
- Documentation must be updated when one or more of a file's volumes are moved.

E2.3 Profile Information (Metadata)

Ministries must maintain profile information for records, volumes and files in order to ensure they can be located. Profile information identifies the unique attributes of records, volumes and files. Attributes include:

- Classification number (the primary-secondary classification)
- Classification title (the primary-secondary title)
- Code and code title, including sub-codes if applicable. Codes differentiate between files with the same classification number in the same office, or are added to a classification number to facilitate retrieval.
- Record date range (the date of the first and last record in each volume of a file, and the first record and last record dates for the entire file)
- Media and/or format (what physical format or formats are the records in?)
- Physical location (where are the records/volumes located? This will include some or all of the following: building, floor, room, shelf or other housing unit, drive, directory, storage media [CD, tape, etc.], container, accession number,

commercial storage facility, or other information relating to the physical location of records and volumes)

- Keywords (words or phrases that allow a user to search for specific files. Depending on technology, keyword searches can be performed by automated records management systems, automated document management systems, automated or manual indexing systems or other methods and tools). Effective keyword searching relies on a controlled vocabulary.

E2.4 Record Maintenance

Files, volumes and records are the components maintained through records management in the BC government.

- A file is not a physical entity. It is the classification and scheduling unit for the records linked to it.
- A volume is a physical entity. It is the physical component of a file.
- A file consists of one or more volumes.
- A volume is maintained in one location.
- Different volumes of one file may be maintained in different locations.
- A volume contains one or more records.
- A record is the indivisible unit for managing recorded information. Records management business requirements do not cover unstructured data or information.

E2.5 Searching For and Retrieving Records

Ministries search for records in order to retrieve and use them. Finding aids must be created and maintained in order to ensure records can be located and retrieved. Finding aids include file lists, box lists, keyword indexes, registers, *ARCS/ORCS* or other attribute information that leads users to the files and records they require. Finding aids may be searched manually or through the use of automated search tools.

E2.6 Access Security

Records in all media or formats must be protected from unauthorized access. This includes records maintained in government offices or on government networks and drives, records maintained in contracted records storage facilities, records maintained on internet or intranet websites, records created by members of the public accessing government services through electronic means, records created by contractors working for government, or other government records maintained in any media or location.

- Access categories must be determined and assigned to record types.
- Access must be restricted in accordance with assigned access categories.
- Designated record documentation (e.g., file lists containing identifying information) must be protected from unauthorised access.
- Records must be protected from unauthorised physical access and unauthorised access through electronic systems.
- Records are located and retrieved by authorised individuals.

E2.7 Transferring Records to Another Location

Records may be transferred from one location to another. A file's volume is the physical entity that is transferred. Hardcopy volumes are physically moved to other locations, and electronic volumes are migrated or transferred. Volumes may be moved within an office, between offices, to and from off-site storage facilities, to and from electronic drives, directories or networks, or temporarily charged out by individuals.

- The new location of a volume must be documented.
- Volumes of one file may be transferred together or individually.
- Accession information must be created and maintained so ministries can locate and access records transferred to off-site storage facilities.

E3 BUSINESS REQUIREMENTS – PRESERVATION MANAGEMENT

Records must be preserved for as long as the provincial government requires them to meet its operational, legal, audit, financial, historical, or other responsibilities. The information maintained on records must also be preserved to ensure it retains its context and authenticity for as long as the government requires the records. Preservation management relates to the physical preservation of record media and the intellectual preservation of recorded information.

E3.1 Physical Preservation of Records

Records must be maintained in a way that protects them from loss, damage, degradation, loss of information, and other threats to their physical integrity and the integrity of the information they contain.

- Records must be maintained on media and in formats that ensure they are readable and accessible for the duration of their active and semi-active retention periods.
- Records scheduled for full or selective retention by the government archives must be maintained on stable media appropriate for permanent retention.
- Records must be housed in environmental conditions that meet their preservation, retrieval and security requirements.
- The record format or media must not compromise the ministry's responsibilities or ability to use the information it contains (e.g., the use of any kind of "lossy" or destructive compression technology that permanently alters the data within the record or datafile, or utilize or introduce additional compression/decompression cycles with data formats that utilise lossy compression techniques).
- Records must be maintained in physical containers appropriate to their media or format.

E3.2 Intellectual Preservation of Records

The context and authenticity of records must be preserved for as long as the government has responsibilities for the information they carry.

- Profile information must be linked to records in a way that ensures they are identifiable and authentic, and the context of their creation and use is maintained.

- Records moved to different media or electronic records moved across carriers must maintain their context and authenticity.

E4 BUSINESS REQUIREMENTS – SCHEDULING MANAGEMENT

Ministries must manage records in accordance with their values. These values are reflected in the retention periods and final dispositions established by *ARCS, ORCS*, and other records retention and disposition schedules. Specific individuals are delegated the authority to apply scheduled retention periods and final disposition to records.

A file is linked to a scheduled retention and disposition schedule through a classification number. A file moves through its life cycle over time, its status changing from active, to semi-active to inactive. The scheduling status of a file is determined by its retention and disposition schedule.

The location of the file's volumes does not affect the file's scheduling status.

All records and volumes of a file follow the same retention period and final disposition.

E4.1 Scheduling Management – Active Records

Active status is the first phase of the file's lifecycle. The retention and disposition schedule that applies to the file determines the length of the active phase.

E4.1.1 Records Classification

A record that has been created or received is classified to a file. The file is linked to the retention and disposition schedule through its classification.

- A record is classified and added to a volume. The volume is linked to the file.
- When a file is classified, the appropriate retention and disposition schedule must be applied to it.
- A file is linked to one retention and disposition schedule.
- A classification is linked to one or more retention and disposition schedules.
- The classification function includes determining the office of primary responsibility (OPR) status of the file.
- Different retention and final disposition schedules may be applied to OPR/non-OPR files.

E4.1.2 Active Status

Active status is the first phase of a file's scheduled life cycle.

- A file is opened when the first record is created and filed.
- A file is active until the end of its scheduled active retention period.

- Active status is designated at the file level and applies to all volumes and records within the file.
- The retention and disposition schedule determines the active retention period.
- The scheduled retention and disposition assigned to a file may be changed during its active phase.

E4.1.3 End of Active Status

Files cease to be active when the scheduled active retention period elapses.

- The active retention period may end after a predetermined period of time, or upon the occurrence of a defined trigger event, or when the ministry makes a decision that the file is no longer required for current usage.
- The end of the scheduled active retention period is the "scheduling date" used to calculate when the file is eligible for final disposition.
- The date of the last record of a file may or may not be the same as the date on which the file's active retention period elapses.
- A file with a semi-active retention period of "nil" (i.e., there is no semi-active retention period) moves to the end of its active and semi-active status at the same time.

E4.2 Scheduling Management – Semi-active Records

When the active retention period elapses, a file's scheduling status changes to semi-active. Semi-active status is designated by the records retention and disposition schedule. Ministries retain their responsibilities for and legal custody of semi-active records.

E4.2.1 Applying Semi-active Retention Schedules

The date the active retention elapses and the file becomes semi-active is called the "scheduling date". This date is used to calculate how long the file is retained and when it is eligible for final disposition.

- The semi-active retention period is determined by the schedule.
- A file must be retained for the entirety of its semi-active retention period.
- A file should not be retained past the end of its semi-active retention period.
- Semi-active retention periods are applied at file level. All volumes within a file will have the same scheduling status and be retained for the same period of time.
- When files are stored in fixed containers, the semi-active retention period is the same for the entire container.
- A semi-active file may be reactivated back to active status.

- The scheduled retention and final disposition of a file can be changed while it is semi-active.

E4.2.2 End of Semi-active Status

Files and file volumes reach the end of their semi-active retention period.

- A file changes status from semi-active to inactive when its semi-active retention period elapses.
- All volumes within a file change status at the same time.

E4.3 Scheduling Management – Inactive Records

When the scheduled semi-active retention period has elapsed, a file reaches inactive status. An inactive file is eligible for scheduled final disposition. The type of final disposition is determined by the records retention and disposition schedule. Final disposition types are:

- destruction,
- transfer to the legal custody of the government archives, or
- alienation of the records from the Crown provincial.

E4.3.1 Applying Final Disposition to Inactive Records

Scheduled final disposition is applied to all volumes of a file. Final disposition should be applied to a file when it is eligible (once it has reached inactive status), unless a halt or hold to final disposition action is required.

- Final disposition actions applied to files must be documented.
- Final disposition action can be halted or deferred if the inactive file is required past its eligible disposition date for litigation or for freedom of information requests.
- A designated individual must authorised final disposition.
- When files are stored in fixed containers, final disposition is applied to the entire container.

Appendix F Desirable System Requirements

Table of Contents

F1. ASSUMPTIONS AND GENERAL REQUIREMENTS 51

F1.1. COTS SOLUTION 51
F1.2. ENTERPRISE-WIDE SCOPE 51
F1.3. INTERFACES WITH OTHER CENTRAL IM APPLICATIONS 52
F1.4. INTEGRATED MANAGEMENT OF ELECTRONIC AND PHYSICAL RECORDS 52

F2. CLASSIFICATION AND SCHEDULING SYSTEM INTERFACE 53

F2.1. ARCS/ORCS DATABASE AND LEGACY SYSTEMS 53

F3. RECORD CREATION AND USE 54

F3.1. CREATING FILES AND VOLUMES 54
F3.2. RECORD CREATION/RECEIPT AND CAPTURE 54
F3.3. REDACTION (CREATION OF RECORD EXTRACTS) 58
F3.4. BATCH IMPORTING 59
F3.5. CLASSIFYING RECORDS 59
F3.6. METADATA 60
F3.7. ORGANIZATIONAL INFORMATION AND LINKAGES 63
F3.8. SEARCHING AND RETRIEVING RECORDS 65
F3.9. TRANSFERRING RECORDS TO ANOTHER LOCATION 67

F4. SCHEDULING MANAGEMENT 68

F4.1. MANAGING RECORDS SCHEDULES 68
F4.2. APPLYING RETENTION PERIODS, INCLUDING REVIEW AND APPROVAL 70
F4.3. DISPOSITION AND TRANSFER/EXPORT 72

F5. PRESERVATION AND ONGOING ACCESS 76

F6. SECURITY 77

F6.1. DELETION OF RECORDS 77
F6.2. RECORDS SECURITY CATEGORIES 78
F6.3. USER ACCESS/AUTHENTICATION 78
F6.4. AUDIT 80
F6.5. BACKUP AND RECOVERY 82
F6.6. VITAL RECORDS 82

F7. PRINTING AND REPORTS 82

F7.1. PRINTING 82
F7.2. REPORTS 83
F7.3. LABELLING 84

F8. ADMINISTRATIVE FUNCTIONS 84

F8.1. GENERAL SYSTEMS ADMINISTRATION 84
F8.2. ADMINISTRATIVE REPORTS 85

F9. DOCUMENT MANAGEMENT 86

F9.1. GENERAL REQUIREMENTS 86
F9.2. INTERACTION WITH RM FUNCTIONS 87

F10. OTHER FUNCTIONALITY 88

F10.1. WORKFLOW 88
F10.2. ELECTRONIC SIGNATURES 90
F10.3. ENCRYPTION 90
F10.4. ELECTRONIC WATERMARKS 91

F11. GENERAL REQUIREMENTS 91

F11.1. EASE OF USE 91
F11.2. PRODUCT MATURITY AND CURRENCY 93
F11.3. SCALABILITY 94
F11.4. PERFORMANCE 95
F11.5. OPENNESS, CONNECTIVITY AND STANDARDS 96

F12. TECHNICAL REQUIREMENTS 98

F12.1. ABILITY TO OPERATE WITHIN BC GOVERNMENT TECHNOLOGY INFRASTRUCTURE 98

F1. Assumptions and General Requirements

The Enterprise Document and Records Management System (EDRMS) will be expected to have the basic characteristics and capabilities outlined below.

The ability of the proposed EDRMS solution to meet these general requirements and other specific requirements will be evaluated on the basis of the responses given in sections F.2 - F.12.

Proponents are asked to check each requirement that the proposed solution can meet. Where narrative responses are requested, Proponents are asked to attach explanatory information.

Note: sources used in compiling these requirements include the:

- *European Commission's Model Requirements for the Management of Electronic Records* ***http://www.cornwell.co.uk/moreq*** ***(cited as MoReq);***
- ***Public Record Office's Functional Requirements for Electronic Records Management Systems*** **http://www.pro.gov.uk/recordsmanagement/eros/invest/default.htm** ***(cited as PRO); and***
- ***Association for Information and Image Management's*** *Implementation Guidelines and Standards Associated with Web-Based Document Management Technologies* ***http://stnds.aiim.wegov2.com/file_depot/0-10000000/0-10000/1462/folder/10666/AIIM+ARP1+2000.pdf*** ***(cited as AIIM)***.

F1.1. COTS Solution

The EDRMS will consist of a single suite of commercial, off the shelf applications covering required document and records management functions for both electronic and physical records, with full integration among application components.

Note: Unless otherwise indicated, the requirements specified in this appendix apply to the EDRMS as a whole. The requirements may be met with a single application or a combination of separate applications (e.g., applications for document management, management of electronic records, and management of physical records, etc.) comprising the integrated EDRMS suite.

F1.2. Enterprise-Wide Scope

For each defined BC government organization (e.g., each ministry), the EDRMS will support integrated management of all common forms of electronic office records (e.g., MS Office and Outlook records) and all forms of hardcopy records. The EDRMS will be extensible to cover other electronic record types (images, database reports, voicemail, etc.).

The EDRMS will support easy transfer of records and records information (metadata) among organizations (e.g., from one ministry to another during government re-organizations).

The EDRMS will enable on-line searching of records information across organizations and across records repositories throughout the BC government.

F1.3. Interfaces with Other Central IM Applications

Records scheduling and classification data is expected to be maintained on a central, government-wide *ARCS/ORCS* database, external to the EDRMS. The EDRMS suite will seamlessly interface with or use the data contained in the *ARCS/ORCS* database for its records classification and scheduling functions.

Data and processes for the management of records stored in offsite facilities (BC Archives Records Centre Services) and the management of archival records will continue to be maintained in the BC Archives ARIS (Archives and Records Information System) application. The EDRMS will maintain specified data described in these requirements that will be drawn from or provided to ARIS and will have the potential for additional future integration with ARIS.

The EDRMS will provide the BC government with a common document and records management infrastructure, integrated with the current standard office applications and infrastructure and with current/emerging document-related applications.

F1.4. Integrated Management of Electronic and Physical Records

The EDRMS will support management of both electronic and physical records in accordance with the existing BC government IM governance requirements (see section 6) and the records management business requirements defined in **Appendix E**.

The EDRMS will enable the authenticity, integrity and accessibility of electronic records to be maintained over time (e.g., decades), across systems (e.g., migrations to new versions of the EDRMS software; export to other systems) and across formats (e.g., export to non-proprietary formats for archival preservation).

The EDRMS will support BC government requirements and processes for the management of physical records and the batch transfer of records containers to central offsite storage facilities and/or BC Archives archival custody.

The EDRMS will maintain standard metadata about electronic and physical files and volumes (including hybrid files consisting of both electronic and physical volumes); will maintain standard metadata about records (i.e., as records profiles); will maintain audit trails of actions taken on records; and will ensure security of records.

F2. Classification and Scheduling System Interface

F2.1. ARCS/ORCS Database and Legacy Systems

F2.1.1. ☐ The EDRMS should use an external master *ARCS/ORCS* database for all records classification data (e.g., primary and secondary data elements) and scheduling data (e.g., records retention periods and disposition categories). The EDRMS should do this by:

F2.1.1.1. ☐ interoperating with the *ARCS/ORCS* database (i.e., incorporate direct "live" connections to the *ARCS/ORCS* tables as part of the EDRMS);

F2.1.1.2. ☐ interfacing with the *ARCS/ORCS* database and downloading required data to the EDRMS as a regular (e.g., monthly), automatic operation requiring minimal data revision in the EDRMS;

F2.1.1.3. ☐ batch importing an initial data set, that must be revised and maintained within the EDRMS; or

F2.1.1.4. ☐ using other means for entering and maintaining *ARCS/ORCS* data within the EDRMS (provide explanation below).

Note: Proponents can evaluate the main types of classification and scheduling data used in ARCS by reviewing ARCS Online ***http://www.bcarchives.gov.bc.ca/arcs/index.htm****. Similar data are used in ORCS and other BC government records schedules.* ***Appendix H*** *provides a brief description of the envisaged structure of the ARCS/ORCS database, planned as central application for developing, reviewing/approving, and electronically publishing the master copies of all ARCS, ORCS and other BC government continuing records schedules.*

F2.1.2. The EDRMS should support use of:

F2.1.2.1. ☐ multiple records classification and scheduling schemes (e.g., multiple *ORCS*) within a single record repository;

F2.1.2.2. ☐ a single records classification and scheduling scheme (e.g., *ARCS* or a single *ORCS*) across a network of electronic record repositories. (Based on MoReq 3.1.9)

F2.1.3. ☐ The EDRMS should support bulk importing of legacy *ARCS/ORCS* scheduling data from existing BC government automated records management systems.

ATTACH AN EXPLANATION OF THE PROPOSED APPROACH FOR MEETING THE ABOVE REQUIREMENTS; E.G.:

- **ABILITY OF THE PROPOSED EDRMS APPLICATION TO MEET THE REQUIREMENT "OUT OF THE BOX";**
- **REQUIRED APPLICATION CUSTOMIZATION;**
- **NATURE OF REQUIRED REVISIONS/MAINTENANCE OF *ARCS/ORCS* DATA WITHIN THE EDRMS;**

- **ANY DATA OR FUNCTIONAL CHARACTERISTICS OF *ARCS/ORCS* WHICH CANNOT BE READILY SUPPORTED BY THE PROPOSED SOLUTION;**
- **ABILITY TO PERFORM REQUIRED *ARCS/ORCS* DEVELOPMENT, MAINTENANCE AND PUBLICATION FUNCTIONS WITHIN THE EDRMS (I.E., ELIMINATING NEED FOR AN EXTERNAL CENTRAL DATABASE);**
- **OTHER RELEVANT CONSIDERATIONS.**

F3. Record Creation and Use

F3.1. Creating Files and Volumes

F3.1.1. ☐ The EDRMS should support the management of records at the file/volume level (hard copy records organized into files/volumes, but not necessarily registered individually) or at the file/volume and record levels (electronic records and hardcopy records that are registered individually).

F3.1.2. ☐ The EDRMS should restrict the entry of new files in the system to authorized users.

F3.1.3. ☐ The EDRMS should support automatic creation of a volume when a file is created.

F3.1.4. ☐ The EDRMS should permit a file to have multiple subordinate volumes.

F3.1.5. ☐ The EDRMS should permit a file to have multiple subordinate volumes open concurrently (i.e., multiple active volumes).

F3.1.6. ☐ The EDRMS should allow an authorised user to re-open a previously closed volume temporarily for the addition of records, and subsequently to close that volume again. (Based on MoReq 3.3.6)

F3.1.7. ☐ The EDRMS should support automatic "roll over" of cyclical files (e.g., files that are closed at the end of a calendar or fiscal year and need to be replaced with new files for the following year covering the same subject matter).

F3.1.8. ☐ The EDRMS should allow for the automatic creation and maintenance of a list (or "repertory") of files. *(*Based on MoReq 3.2.10)

F3.1.9. ☐ The EDRMS should define in the file repertory physical files and volumes, and should allow the presence of physical records in these volumes to be reflected and managed in the same way as electronic records. *(*Based on MoReq 10.1.1)

F3.1.10. ☐ The EDRMS should support the management of "hybrid" files containing electronic and physical components, and allow the components to be managed in an integrated manner. *(*Based on MoReq 10.1.2)

F3.1.11. ☐ The EDRMS should allow a different metadata element set to be configured for physical files and electronic files; physical file metadata should include information on the physical location of the physical file. *(*Based on MoReq 10.1.4)

F3.2. Record Creation/Receipt and Capture

F3.2.1. The EDRMS should enable documents to be captured as records by assigning records registration numbers and establishing profile metadata for the records.

F3.2.1.1. ☐ The EDRMS should support the registration of electronic records.

F3.2.1.2. ☐ The EDRMS should support the registration of physical records.

F3.2.1.3. ☐ The EDRMS should be capable of creating profiles for electronic records.

F3.2.1.4. ☐ The EDRMS should be capable of creating profiles for physical records.

F3.2.2. The EDRMS capture process should provide the functionality to:

F3.2.2.1. ☐ register and manage all electronic records regardless of the method of encoding or other technological characteristics;

F3.2.2.2. ☐ ensure that the records are associated with a classification scheme and can be associated with one or more files;

F3.2.2.3. ☐ integrate with the application software that generates the records (where possible);

F3.2.2.4. ☐ validate and control the entry of metadata into the EDRMS. *(*Based on MoReq 6.1.1).

F3.2.3. The EDRMS should capture in the electronic records management environment:

F3.2.3.1. ☐ the content of the electronic record, including information defining its form and rendition and information defining the structure and behaviour of the electronic record, retaining its structural integrity (for example, all the components of an e-mail message with attachment(s), or of a web page, with their links);

F3.2.3.2. ☐ information about the electronic document, for example, the file name;

F3.2.3.3. ☐ the date of creation and other document metadata about the elements of the record;

F3.2.3.4. ☐ information about the context in which the electronic record was originated, created and registered, for example its business process and, originator(s), author(s);

F3.2.3.5. ☐ information about the application program, which generated the record, including its version. *(*Based on MoReq 6.1.2)

F3.2.4. ☐ The EDRMS should allow the capture acquisition of metadata elements specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times. *(*Based on MoReq 6.1.3)

F3.2.5. ☐ The EDRMS should ensure authorized users and administrators only can change the content of selected elements of the metadata of the electronic record. *(*Based on MoReq 6.1.4)

F3.2.6. ☐ The EDRMS should support the ability to assign the same electronic records to different electronic files, from one electronic document without physical duplication of the electronic record. *(*Based on MoReq 6.1.5)

F3.2.7. ☐ The EDRMS should support automated assistance in registration of electronic documents, by automatically extracting metadata for as many types of documents as possible, including at least the following document types:

F3.2.7.1. ☐ office documents (e.g., word-processed letters in a standard format);

F3.2.7.2. ☐ e-mail without attachments, both incoming and outgoing;

F3.2.7.3. ☐ e-mail with attachments, both incoming and outgoing;

F3.2.7.4. ☐ facsimile messages, both incoming and outgoing. *(*Based on MoReq 6.1.6; 6.1.14)

F3.2.8. ☐ The EDRMS should record the date and time of registration as metadata. *(*Based on MoReq 6.1.7)

F3.2.9. ☐ The EDRMS should ensure that every registered record has a viewable registry entry that includes metadata specified at configuration time. *(*Based on MoReq 6.1.8)

F3.2.10. ☐ The EDRMS should allow entry of further descriptive and other metadata at the time of registration and/or at a later stage of processing. *(*Based on MoReq 6.1.9)

F3.2.11. Where a document has more than one version, the EDRMS should allow users to choose at least one of the following:

F3.2.11.1. ☐ register one version of the document as a record;

F3.2.11.2. ☐ register each version of the document as a record;

F3.2.11.3. ☐ register all versions of the document as one record. *(*Based on MoReq 6.1.10)

F3.2.12. ☐ The EDRMS should allow a user to pass electronic records to another user to complete the process of capture. *(*Based on MoReq 6.1.12)

F3.2.13. For electronic records that are constructed of more than one component, the EDRMS should provide the following functions:

F3.2.13.1. ☐ handle the record as a single indivisible record, retaining the relationship between the components;

F3.2.13.2. ☐ retain the record's structural integrity;

F3.2.13.3. ☐ support later integrated retrieval, display, management;

F3.2.13.4. ☐ manage disposal of all components of the electronic record as a whole unit (i.e., in one operation). *(*Based on MoReq 6.1.13)

F3.2.13.5. ☐ The EDRMS should issue a warning if a user attempts to register a document that has already been registered in the same file. *(*Based on MoReq 6.1.15)

F3.2.14. ☐ The EDRMS should support the capture of common forms of BC government office documents as records. These include both simple and compound document format types; e.g.:

F3.2.14.1. ☐ Simple: wp documents, presentations, spreadsheets (at minimum, all MS Office document types); e-mail messages (at minimum, MS Outlook); text, images, facsimiles ;

F3.2.14.2. ☐ Compound: electronic mail with attachments, desktop publishing, web pages, graphics, "layered" documents generated from database or GIS applications. (Based on MoReq 6.3.2)

F3.2.15. ☐ The EDRMS should support the ability to capture completed forms, including both the form content and the original structure of the form at the time of data entry.

F3.2.16. ☐ The document formats supported should be extendable as new formats are introduced. (Based on MoReq 6.3.3)

F3.2.17. The EDRMS should be able to capture the following types of documents:

F3.2.17.1. ☐ electronic calendars;

F3.2.17.2. ☐ information from other computer applications e.g., Accounting, Payroll, Computer Aided Design, GIS;

F3.2.17.3. ☐ scanned paper documents;

F3.2.17.4. ☐ voice files;

F3.2.17.5. ☐ video clips;

F3.2.17.6. ☐ digital schematics and maps;

F3.2.17.7. ☐ structured data (e.g., EDI transactions);

F3.2.17.8. ☐ databases;

F3.2.17.9. ☐ multimedia documents. *(*Based on MoReq 6.3.4)

F3.2.18. ☐ The EDRMS should not impose any practical limit on the number of records, which can be captured in a file, or on the number of records, which can be stored in the EDRMS. *(*Based on MoReq 6.3.5)

F3.2.19. The EDRMS should allow a compound document to be captured in either of two ways:

F3.2.19.1. ☐ as a single compound record;

F3.2.19.2. ☐ as a series of linked simple records, one per component of the compound document. *(*Based on MoReq 6.3.6)

F3.2.20. ☐ The EDRMS should provide seamless integration with, and continued support for, existing document creation and filing tools, such as MS Word and Windows Explorer, etc.

F3.2.20.1. ☐ For example, when using MS Word/Explorer, etc. with records in the EDRMS repository, the File Open command should result in check-out; the File Save command should result in check in.

F3.2.20.2. ☐ The EDRMS should allow users to process and capture their incoming e-mail messages from within their e-mail system. The user should be able to process each e-mail in the inbox, from within their e-mail system, as follows:

F3.2.20.3. ☐ view each mail message and an indication of its attachments (if any);

F3.2.20.4. ☐ view the contents of the attachments using multi-format document viewer;

F3.2.20.5. ☐ register the mail message and its attachments as a new record in EDRMS;

F3.2.20.6. ☐ link the mail message and its attachments to an existing record in EDRMS. *(*Based on MoReq 6.4.2).

F3.3. Redaction (Creation of Record Extracts)

It is sometimes necessary to make available records containing sensitive information. In such cases, there may be a need to remove the sensitive information, without affecting the underlying record. The process is referred to here as redaction, and the EDRMS should store both the original record and the redacted copy, which is called an 'extract' of the record.

F3.3.1. ☐ The EDRMS should allow authorized users to take a copy of a record, for the purposes of redaction. *(*Based on MoReq 9.3.9)

F3.3.2. The EDRMS should provide functionality for removing or hiding sensitive information from the extract, to include at least:

F3.3.2.1. ☐ removal of individual pages of a multi-page image record;

F3.3.2.2. ☐ addition of opaque rectangles to obscure sensitive names or words

F3.3.2.3. ☐ other means of hiding or extracting sensitive information;

F3.3.2.4. ☐ any other features required for video or audio formats if present. *(*Based on MoReq 9.3.10)

F3.3.3. ☐ If the proposed EDRMS does not provide the above functionality, it should integrate with other software packages to do so. *(*Based on MoReq 9.3.10)

F3.3.4. ☐ The EDRMS should ensure that none of the removed or hidden information could ever be seen in the extract. *(*Based on MoReq 9.3.10)

F3.3.5. ☐ When an extract is created, the EDRMS should record its creation in the record's metadata, including at least date, time, reason for creation and creator. *(*Based on MoReq 9.3.11)

F3.3.6. ☐ The EDRMS should prompt the creator of an extract to assign it to a file. *(*Based on MoReq 9.3.12)

F3.3.7. ☐ The EDRMS should store a cross-reference to an extract in the same file and volume as the original record, even if that file volume is closed. *(*Based on MoReq 9.3.13)

F3.4. Batch Importing

F3.4.1. The EDRMS should provide the capability for authorized individuals to bulk load, as a minimum, pre-existing:

F3.4.1.1. ☐ file and volume records;

F3.4.1.2. ☐ electronic records;

F3.4.1.3. ☐ records profiles.

F3.4.2. ☐ The EDRMS should provide the ability to capture transactional documents generated by other systems. This should include:

F3.4.2.1. ☐ supporting predefined batch file transaction imports;

F3.4.2.2. ☐ providing edit rules to customize the automatic registration of the records;

F3.4.2.3. ☐ maintaining data integrity validation. *(*Based on MoReq 6.2.1)

F3.4.3. ☐ The EDRMS system should provide facilities to manage input queues. *(*Based on MoReq 6.2.2)

F3.4.4. ☐ The EDRMS should be able to set up multiple input queues for different document types. *(*Based on MoReq 6.2.3)

For example, in different environments, queues might be for e-mails, scanned correspondence, documents from a department, group or individual, transactions from computer applications, or documents from other document/content management systems.

F3.5. Classifying Records

F3.5.1. ☐ The EDRMS should be capable of ensuring that all records are classified and scheduled in accordance with the established *ARCS/ORCS* classification schemes.

F3.5.2. ☐ The EDRMS should allow user determination of classifications applied to records when they are classified and registered into the system. The system should provide classification assists for users including some or all of the following:

F3.5.2.1. ☐ making subsets of classification schemes accessible to users or roles;

F3.5.2.2. ☐ storing lists of recently used classifications or files for users or roles;

F3.5.2.3. ☐ suggesting the most recently used classifications or files by users;

F3.5.2.4. ☐ suggesting classifications or files that contain related electronic records;

F3.5.2.5. ☐ suggesting classifications or files by inference drawn from record metadata elements; for example, significant words used in the document title;

F3.5.2.6. ☐ suggesting classifications or files by inference from record contents. *(*Based on MoReq 6.1.11)

F3.5.3. ☐ The EDRMS should provide an "intelligent" engine for the above classification/filing suggestions that can:

F3.5.3.1. ☐ "learn" from past choices made by the user and improve it's ability to suggest correct classifications or files

F3.5.3.2. ☐ be configured to auto-classify/auto-file records when a user-specified accuracy level is achieved (e.g., auto-classify if a specified accuracy level is possible, otherwise flag for manual classification).

F3.5.4. ☐ The EDRMS should permit users to move easily between the classification schemas (e.g., primary and secondary records) and lists of existing files when determining appropriate classifications.

F3.5.5. ☐ The EDRMS should identify any existing files under a chosen classification.

F3.5.6. ☐ The EDRMS should permit the reclassification of records or files. If a file is reclassified, the EDRMS should ensure the revised data cascades to volumes and, if required, records.

F3.5.7. ☐ The EDRMS should support the classification or reclassification of multiple files in one operation.

F3.5.8. ☐ The EDRMS should allow users to create cross-references (e.g., "see also" type links) between related files. (Based on MoReq 3.4.11)

F3.6. Metadata

F3.6.1. ☐ The EDRMS should support the designation of metadata by authorized users/administrators.

F3.6.2. ☐ The EDRMS should allow specific sets of metadata elements to be defined for different kinds of records at configuration time. *(*Based on MoReq 12.1.3)

F3.6.3. ☐ The EDRMS should restrict the ability to make changes to metadata values to authorized users.

F3.6.4. ☐ The EDRMS should support the recording of file and volume metadata when a file is created.

F3.6.5. ☐ The EDRMS should support the entry of the types of file/volume metadata specified at **Appendix G.3**.

F3.6.6. In particular, file/volume metadata should include:

F3.6.6.1. ☐ file first record date and file last record date (the date range of the file contents; ideally, cascaded up from volume date ranges);

F3.6.6.2. ☐ volume first and last record dates (the date range of the records within the volume);

F3.6.6.3. ☐ file schedule trigger date; i.e., the date from which the eligible disposition date is calculated. It should be possible for the schedule trigger date to be different than the file last record date or the file closure date.

F3.6.7. ☐ The EDRMS should support bulk updates of profile information based on specified criteria. The EDRMS should support batch input and acquisition of profile information (e.g., to a series of files, or a group of records, or multiple volumes of a file).

F3.6.8. ☐ The EDRMS should not present any practical limitation on the number of metadata elements allowed for each item (e.g., file, volume, record). *(*Based on MoReq 12.1.1)

F3.6.9. ☐ Where the contents of a metadata element can be related to the functional behavior of the EDRMS, the EDRMS should use the contents of that element to determine the functionality. *(*Based on MoReq 12.1.2)

For example, if the EDRMS stores security categories of records and also stores the security clearance of users, then it should use the latter to determine whether a user can or cannot access a record. If the EDRMS only stores the clearances and categories as text fields which are not used to control access, this requirement is not met.

F3.6.10. The EDRMS should support at least the following metadata element formats:

F3.6.10.1. ☐ alphabetic;

F3.6.10.2. ☐ alphanumeric;

F3.6.10.3. ☐ numeric;

F3.6.10.4. ☐ date;

F3.6.10.5. ☐ logical (i.e., yes/no, true/false). *(*Based on MoReq 12.1.5).

F3.6.11. ☐ The EDRMS should support the ability to extract metadata elements automatically from records when they are captured. *(*Based on MoReq 12.1.9)

Examples are the automatic extraction of dates, titles, recipient names and reference numbers from word processed documents or structured transaction documents such as invoices.

F3.6.12. ☐ The EDRMS should allow the Administrator to define at configuration time whether each metadata element is mandatory or optional and whether it is searchable. *(*Based on MoReq 12.1.4)

F3.6.13. ☐ Where metadata element values are entered manually, the EDRMS should support persistent default values, which are user-definable. (Based on MoReq 12.1.16)

A persistent default appears as the default in the data entry field for each item in succession until a user changes it. Once changed, the new value remains, i.e., becomes persistent.

F3.6.14. ☐ The EDRMS should allow configuration such that any metadata element can be used as a search field in a non-structured search (e.g., a free text search). *(*Based on MoReq 12.1.17)

F3.6.15. The EDRMS should be able to acquire metadata from:

F3.6.15.1. ☐ the document-creating application package or operating system or network software;

F3.6.15.2. ☐ the user at the time of capture or registration;

F3.6.15.3. ☐ rules defined at configuration time for generation of metadata by the EDRMS at the time of registration. *(*Based on MoReq 12.1.22)

F3.6.16. ☐ The EDRMS should allow the values of metadata to be provided automatically from the next higher level in the classification scheme hierarchy. *(*Based on MoReq 12.1.11)

For example, for a volume, the value of some of the metadata elements should be inherited from its parent file; and for a record, the value of some metadata may be inherited from the volume into which it is stored.

F3.6.17. ☐ When changes are made to the *ARCS/ORCS* database that affect file-level information, the EDRMS should support a prompt that flags changes, and requires authorized approval to initiate the cascade.

F3.6.18. ☐ The EDRMS should support validation of metadata when users enter the metadata, or when it is imported. Validation should use at least the following mechanisms:

F3.6.18.1. ☐ format of the element contents;

F3.6.18.2. ☐ range of values;

F3.6.18.3. ☐ validation against a list of values maintained by the Administrator;

F3.6.18.4. ☐ a valid classification scheme reference. *(*Based on MoReq 12.1.13)

An example of format validation is that the contents are all numeric, or are in a date format (Based on MoReq 12.1.5)

An example of range format validation is that the contents fall in the range between 1 January 1999 and 31 December 2001. An example of validation against a list of values is verifying that an export destination is present on a list.

F3.6.19. ☐ The EDRMS should support validation of metadata elements using check digit algorithms. *(*Based on MoReq 12.1.14)

For example, files may be identified by a sixteen-digit credit card number, of which the last digit is a check digit computed from the other fifteen digits using the mod 10 algorithm. Provision of

an application program interface for this feature, allowing organisations to introduce their chosen algorithm, should normally be considered acceptable.

F3.6.20. ☐ The EDRMS should, where required, support validation of metadata using calls to another application (e.g., to a personnel system to check whether a personnel number has been assigned, or to a postal code database system). *(*Based on MoReq 12.1.15)

F3.6.21. ☐ The EDRMS should ensure that volumes and records retain their unique identification regardless of location or scheduling status. E.g.:

F3.6.21.1. ☐ volumes batched within an accession for offsite transfer should retain their individual identity in the batch and it should be possible to remove the volumes from the accession without undue effort.

F3.6.22. ☐ The EDRMS should support BC Archives records centre processes for transferring physical records to off-site storage facilities. For example, it should support the entry of the types of off-site transfer metadata specified at **Appendix G.4**.

F3.6.23. In particular, offsite transfer metadata should include:

F3.6.23.1. ☐ accession number (7 digit number assigned that identifies one or more batches of containers/volumes transferred offsite; number is generated by BC Archives ARIS system) ;

F3.6.23.2. ☐ application number (6 digit service application number identifies a particular batch of containers/files transferred offsite under an accession number; number is issued on BC Archives service application forms);

F3.6.23.3. ☐ container number (10 digit number; comprised of the 6 digit accession number followed by a 4 digit box number; e.g. 920345-0013).

F3.6.24. ☐ Once physical volumes are boxed, the EDRMS should support a simple method of recording the container number in the metadata for each boxed volume (i.e., ability to select multiple volumes and record the box number in a single operation).

F3.7. Organizational Information and Linkages

F3.7.1. ☐ The EDRMS should be able to use the ARIS name authority tables (see **Appendix H.4**) as a control source for organizational names. The EDRMS should do this by:

F3.7.1.1. ☐ interoperating with the ARIS tables;

F3.7.1.2. ☐ interfacing with the ARIS tables and downloading required data to the EDRMS as a regular (e.g., monthly), automatic operation requiring minimal data revision in the EDRMS;

F3.7.1.3. ☐ batch importing an initial data set, that must be revised and maintained within the EDRMS; or

F3.7.1.4. ☐ using other means for entering and maintaining ARIS name records within the EDRMS.

F3.7.1.5. ☐ At minimum, the EDRMS should be capable of associating ARIS name ID numbers (8 digit numeric field) with name records maintained within the EDRMS.

Note: The following requirements apply whether the EDRMS utilises ARIS name records or uses another method to maintain a controlled source of organisational names.

F3.7.2. ☐ The EDRMS should be able to identify BG government organizational units and the responsibilities/roles they hold/perform for particular records or groups of records (e.g., records legal custodian, records creator, Office of Primary Responsibility (OPR)).

F3.7.3. ☐ The EDRMS should be able to maintain/use multi-level name records for BC government organizations down to at least 8 levels; e.g., a record for each ministry, division, branch, section, unit, office, etc., ideally with each name record:

F3.7.3.1. ☐ linked to the higher and lower level name in a parent/child relationship;

F3.7.3.2. ☐ linked to predecessor and successor names to track changing organizational structures over time.

F3.7.4. ☐ The EDRMS should be able to use the organizational name records to provide the types of organizational metadata elements specified in **Appendix G**; e.g.:

F3.7.4.1. ☐ current legal custodian (owner), creator, and/or OPR names for files/volumes/records

F3.7.4.2. ☐ transferring agent names for applications/accessions (names of offices transferring batches of records to offsite storage)

F3.7.5. ☐ The EDRMS should support the assignment of files to an organizational unit (e.g., identifying the organization as having legal custody or other specified responsibility for the files).

F3.7.6. ☐ The EDRMS should enable users to specify and use generic terms (e.g., central office, field office) to identify OPRs or other organizational responsibilities, where it is not feasible to use a specific organization name.

F3.7.7. ☐ The EDRMS should support efficient bulk moves of files/volumes/records and their metadata from one organizational unit to an inheriting organizational unit.

F3.7.8. ☐ The EDRMS should support batch changes of organizational metadata (e.g., changes to the name of the current legal custodian for files/records transferred from one organization to another).

F3.7.9. ☐ If there is a change of legal custody, the EDRMS should ensure organizational metadata for files/volumes/records is updated while maintaining a history of past legal custodians.

F3.7.10. ☐ The EDRMS should allow Administrators to make changes to the organizational name records and file repertory, ensuring all metadata and audit trail data are handled correctly and completely at all times, in order to reflect the following kinds of organizational change:

F3.7.10.1. ☐ division of an organizational unit into two or more units;

F3.7.10.2. ☐ combination of two or more organizational units into one;

F3.7.10.3. ☐ movement or re-naming of an organizational unit;

F3.7.10.4. ☐ division of a whole organization into two or more organizations. *(*Based on MoReq 9.1.6)

F3.7.10.5. ☐ The EDRMS should support the movement of User IDs between organizational units, and any changes to access authority. *(*Based on MoReq 9.1.7)

F3.8. Searching and Retrieving Records

This section describes the functionality required to search for records and/or their metadata, and to display the records/metadata.

Searching

F3.8.1. The EDRMS should support enterprise-wide searching; i.e., a user with the requisite permissions should be able to conduct:

F3.8.1.1. ☐ searches of the records of an entire organizational unit

F3.8.1.2. ☐ *concurrent* searches of records across multiple organization units and/or records repositories (e.g., users do not need to conduct separate searches for each organization unit or repository but rather can search across an entire ministry or across multiple ministries).

F3.8.2. ☐ The EDRMS search mechanisms should be integrated and should, to users, appear the same for all classification levels. *(*Based on MoReq 8.1.2)

In other words, users should see the same interface, features and options whether searching for ARCS/ORCS classifications, files or records.

F3.8.3. ☐ The EDRMS should support searches of the classification system.

F3.8.4. ☐ The EDRMS should allow the metadata of any object (such as record, volume, file or primary and secondary) to be searched, using the techniques in this section. (Based on MoReq 8.1.19)

F3.8.5. ☐ The EDRMS should support searches of profiles of both physical and electronic records.

F3.8.6. ☐ The EDRMS should search records profiles regardless of the location (e.g., online or off-line) or scheduling status (e.g., active or semi-active) of the records. *(*Based on MoReq 8.1.19)

F3.8.7. ☐ In the case of files, the EDRMS should present seamless functionality across searches for electronic files, hybrid files and physical files. *(*Based on MoReq 8.1.3)

F3.8.8. ☐ The EDRMS should allow the user to set up a single search request with combinations of metadata and/or record content. *(*Based on MoReq 8.1.6)

F3.8.9. The EDRMS should provide searching tools that cover the following techniques:

F3.8.9.1. ☐ free text searching of combinations of record and file metadata elements and record content;

F3.8.9.2. ☐ Boolean searching of metadata elements. *(*Based on MoReq 8.1.8)

F3.8.10. ☐ The EDRMS should provide concept searching by the use of a thesaurus incorporated as an on-line index. *(*Based on MoReq 8.1.10)

F3.8.11. ☐ The EDRMS should provide for "wild card" searching of metadata that allows for forward, backward and embedded expansion. *(*Based on MoReq 8.1.11)

F3.8.12. ☐ The EDRMS should provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a hit. (Based on MoReq 8.1.12)

F3.8.13. ☐ The EDRMS should provide browsing mechanisms that provides graphical or other display browsing techniques at the classification, file/volume and records levels (including selection, retrieval and display of electronic files and their contents). *(*Based on MoReq 8.1.13)

F3.8.14. ☐ The EDRMS should allow users to save and re-use queries. *(*Based on MoReq 8.1.20)

F3.8.15. ☐ The EDRMS should allow users to refine (i.e., narrow) searches. *(*Based on MoReq 8.1.21)

F3.8.16. ☐ The EDRMS should allow the use of named time intervals in search requests, e.g., "last week", "this month". *(*Based on MoReq 8.1.22)

F3.8.17. ☐ The EDRMS should provide relevance ranking of the search results. *(*Based on MoReq 8.1.25)

F3.8.18. ☐ When viewing or working with a record or aggregation (e.g., file or class) of records, whether as the result of a search or not, a user should be able to use EDRMS features to find information about the next-higher level of aggregation of records easily and without leaving or closing the record. *(*Based on MoReq 8.1.27)

For example, when reading a record, the user should be able to find out what volume and file it is in; if viewing file metadata, the user should be able to find out information about the primary-secondary in which it is located.

Display/Retrieval

An EDRMS may contain records with different formats and structures. The user requires generic viewing facilities that will accommodate rendering (displaying) a range of formats.

F3.8.19. ☐ The EDRMS should render records retrieved from searches. *(*Based on MoReq 8.2.1).

If the EDRMS is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the EDRMS.

F3.8.20. The EDRMS should provide display formats, configurable by users, for search results having the functions listed below. *(*Based on MoReq 8.1.24)

F3.8.20.1. ☐ select the order in which the search results are presented;

F3.8.20.2. ☐ specify the number of hits displayed on the screen per view from the search;

F3.8.20.3. ☐ set the maximum number of hits for a search;

F3.8.20.4. ☐ save the search results;

F3.8.20.5. ☐ choose which metadata fields are displayed in search result lists.

F3.8.21. ☐ The EDRMS should display the total number of hits from a search on the user's screen and should allow the user to then display the search results (the "hit list"), or refine his or her search criteria and issue another request. *(*Based on MoReq 8.1.17)

F3.8.22. ☐ The EDRMS should allow records, files etc. listed in a hit list to be selected then opened (subject to access controls) by a single click or keystroke. *(*Based on MoReq 8.1.18)

F3.8.23. ☐ The EDRMS should be able to search for and retrieve a complete electronic file, or file volume, and all its contents and contextual metadata, and render all, and only, those entries in the context of that file as a discrete group and in a single retrieval process. *(*Based on MoReq 8.1.15)

F3.8.24. ☐ The EDRMS should render records that the search request has retrieved without loading the associated application software. *(*Based on MoReq 8.2.2).

F3.8.25. ☐ The EDRMS should be able to render all the types of electronic records specified by the organization in a manner that preserves the information of the records (e.g., all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record together. *(*Based on MoReq 8.2.3).

F3.8.26. ☐ The EDRMS should ensure that retrieval of a hybrid file retrieves the metadata for both electronic and paper records associated with it. *(*Based on MoReq 10.1.6)

F3.9. Transferring Records to Another Location

Transferring records to another location implies the movement of file volumes on-site within or between ministries; it does not refer to transferring files to off-site storage facilities or to the custody of the BC Archives (for the latter, see Scheduling Management)

F3.9.1. ☐ The EDRMS should provide a tracking feature to monitor and record information about the location and movement of volumes, both electronic and physical. *(*Based on MoReq 4.4.1).

F3.9.2. The tracking function should record information about movements that includes the following:

F3.9.2.1. ☐ unique identifier of the file or records;

F3.9.2.2. ☐ current location as well as a user-defined number of previous locations (locations should be user-defined);

F3.9.2.3. ☐ date file sent/moved from location;

F3.9.2.4. ☐ date file received at location (for transfers);

F3.9.2.5. ☐ user responsible for the move (where appropriate). *(*Based on MoReq 4.4.2).

F3.9.3. ☐ The EDRMS should support tracking of physical volumes by the provision of checkout, check-in and bring forward facilities, which reflect the current location of the volume. *(*Based on MoReq 10.1.5)

F3.9.4. ☐ The EDRMS should support on-line requests to reserve file volumes for future sign out; e.g., user or adminstrator to link bring forward criteria to a record (person requesting bring forward, due date, action to be taken, etc.).

F3.9.5. ☐ The EDRMS should handle multiple bring forwards from different sources concurrently.

F3.9.6. ☐ The EDRMS should support volume-level location controls for physical volumes.

F3.9.7. ☐ The EDRMS should support individual or bulk updates of location profile information.

F4. Scheduling Management

One of the primary purposes of the EDRMS is to automate the retention and disposition of electronic records and to facilitate the retention and disposition of records in traditional media. Retention periods and disposition decisions are identified in records schedules, such as *ARCS* or *ORCS*.

Requirements for establishing, maintaining, and calculating retention periods are listed in Section B.4.1. Requirements for the processes that take place at the date specified by the retention periods are described in subsequent sections.

Requirements for review and approval processes are listed in Section B.4.2, and requirements for transfer, export and destruction are listed in Section B.4.3.

F4.1. Managing Records Schedules

F4.1.1. ☐ The EDRMS should provide a function that specifies retention schedules, calculates retention periods and eligible disposition dates, automates reporting and destruction actions, and provides integrated facilities for exporting records and metadata. *(*Based on MoReq 5.1.1)

F4.1.2. ☐ Every record of a file should be governed by the retention period(s) associated with that file.

F4.1.3. ☐ EDRMS should provide functionality to enable all components of a file to be retained and disposed of as a unit, even if volumes are maintained in different locations and/or in different media and formats, for example, “hybrid” files.

F4.1.4. For each file, the EDRMS should:

F4.1.4.1. ☐ automatically track retention periods that have been allocated to the file;

F4.1.4.2. ☐ initiate the disposal process once the end of the retention period is reached. *(*Based on MoReq 5.1.8)

F4.1.5. ☐ The EDRMS should be capable of associating more than one retention period with any secondary of the classification scheme.

For example, each secondary in ARCS/ORCS is associated with two retention periods: one for the office of primary responsibility (OPR) and one for the non-office of primary responsibility (non-OPR). In addition, there may be a special schedule (such as the Executive Records Schedule) that is associated with an organizational unit or particular category of record that will override the retention periods defined in ARCS/ORCS.

F4.1.6. ☐ The EDRMS should allow organization units to use one or more schedules simultaneously (for example, *ARCS* and one or more *ORCS*).

F4.1.7. ☐ The EDRMS should allow authorized users to change or amend any retention period allocated to any file at any point in the life of the file. *(*Based on MoReq 5.1.15)

F4.1.8. ☐ EDRMS should require determination of a file’s OPR status when the file is classified.

F4.1.9. ☐ The Administrator should have the option to restrict the choice of OPR or non-OPR retention periods for specified secondaries (e.g., the Payroll office will have only the OPR option for Employee Pay Files, while all other offices will have only the non-OPR option).

F4.1.10. ☐ EDRMS should allow the Administrator to designate an org unit as governed by a special schedule or defining an aggregation of files as governed by a special schedule, regardless of classification numbers applied to file(s).

F4.1.11. ☐ When an Administrator moves files or records between secondaries of the classification scheme, the EDRMS should optionally allow the retention period of the destination secondary to replace the existing retention period(s) applying to these records. *(*Based on MoReq 5.1.18)

F4.1.12. ☐ The EDRMS should support reporting and analysis tools for the management of retention and disposition schedules by the Administrator, including the ability to:

F4.1.12.1. ☐ list all retention schedules;

F4.1.12.2. ☐ list all files to which a specified retention schedule is assigned. *(*Based on MoReq 5.2.8)

F4.1.13. ☐ The EDRMS should support retention periods that are based on time (such as a calendar year or a fiscal year), trigger events (known as “superseded or obsolete” or “SO”), or time – event retentions (superseded or obsolete plus a period of time).

F4.1.14. ☐ The EDRMS should support retention periods of time from one month to one hundred years. *(*Based on MoReq 5.1.12)

F4.1.15. ☐ The EDRMS should calculate retention period for the file based on "scheduling date". The "scheduling date" may be the date upon which a defined cycle ends (e.g., March 31), or the date upon which a trigger event occurs (e.g., Contract ends), or a decision is made (e.g., information no longer required).

F4.1.16. The EDRMS should allow at least the following decisions for each retention period:

F4.1.16.1. ☐ retain indefinitely;

F4.1.16.2. ☐ present for review at a future date, as defined below;

F4.1.16.3. ☐ destroy at a future date, as defined below;

F4.1.16.4. ☐ transfer at a future date, as defined below. *(*Based on MoReq 5.1.10)

F4.1.17. ☐ Each retention schedule should allow the retention periods to be specified for a future date, with the date being specified in at least the following ways:

F4.1.17.1. ☐ passage of a specified period of time after the file is opened;

F4.1.17.2. ☐ passage of a specified period of time after the file is closed;

F4.1.17.3. ☐ elapse of a specified interval since assignment of the last record to the file;

F4.1.17.4. ☐ elapse of a specified interval since a record was retrieved from the file;

F4.1.17.5. ☐ elapse of a specified interval since a specific event described in the schedule that results in a notification being sent to the EDRMS from the Administrator (rather than being detected automatically by the EDRMS). (Based on MoReq 5.1.11)

While the above is generally inclusive, it is possible that some kinds or records will have types of retention requirements not listed here.

F4.1.18. ☐ The EDRMS should, by default, prevent the user from adding electronic records to a closed file.

F4.1.19. ☐ The EDRMS should permit authorized users to suspend the retention period and final disposition of a file(s). The suspension ("hold") is applied at the file level and affects all components of the file.

F4.1.19.1. ☐ EDRMS should permit authorized users to lift "holds."

F4.1.19.2. ☐ EDRMS should support the placing or lifting of holds on single files and/or classes of files.

F4.2. Applying Retention Periods, Including Review and Approval

The records officer is required to review and approve any transfer or disposition actions to ensure that users are using the retention schedules correctly. The EDRMS should have

functionality to assist users in determining which records are ready for transfer or disposal, and to assist records officers in reviewing the application of records schedules.

F4.2.1. ☐ The EDRMS should support the creation of reports ("pull lists") listing all open files that have reached the end of their active retention period and are eligible for transfer or disposition. These lists should be organized to facilitate boxing of physical files, that is, by final disposition date and final disposition action (e.g., selective/full retention or destruction).

F4.2.2. ☐ The EDRMS should allow volumes to be transferred off-site even if they are still active.

F4.2.3. ☐ The EDRMS should allow for closed files/volumes in off-site storage to be reactivated, or permanently removed from a box and re-entered into the active records management system.

F4.2.4. ☐ The EDRMS should support box/container management functions, such as:

F4.2.4.1. ☐ calculating the eligible disposition date for the box/container based upon the file with the longest retention period in the box; or

F4.2.4.2. ☐ recalculating the eligible disposition date should any files be permanently removed from the box/container.

F4.2.5. ☐ The EDRMS should allow the definition of sets of processing rules to be applied as an alerting facility to specified files, prior to initiation of the disposal process. Specific requirements should include the following:

F4.2.5.1. ☐ managers and Administrators should be able to review files and contents;

F4.2.5.2. ☐ the EDRMS should notify the Administrator of files with a given security level.

F4.2.6. ☐ The EDRMS should be able to notify the Administrator regularly of all retention periods that will come into force in a specified period of time, and provide quantitative reports on the volumes and types of records. (Based on MoReq 5.2.1)

F4.2.7. ☐ The Administrator should be able to specify the frequency of a retention period report, the information reported and highlighting exceptions such as disposal overdue. (Based on MoReq 5.2.2)

F4.2.8. ☐ The EDRMS should support the review process by presenting electronic files to be reviewed, with their metadata and retention schedule information (the reason), in a manner which allows the reviewer to browse (i.e., navigate and study) the file contents and/or metadata efficiently. (Based on MoReq 5.2.3)

In practice, this implies features for navigating forward, back etc. within and between files, and from/to the metadata for files and records.

F4.2.9. ☐ The EDRMS should alert the Administrator if an electronic file/record that is due for destruction is referred to in a link from another file/record; and should pause the destruction process to allow the following remedial actions to be taken:

F4.2.9.1. ☐ confirmation by the Administrator to proceed with or cancel the process; and

F4.2.9.2. ☐ the generation of a report detailing the files or records and all references or links for which it is a destination. *(*Based on MoReq 5.2.4)

F4.2.10. The EDRMS should allow the reviewer to take at least any of the following actions for each file during review:

F4.2.10.1. ☐ mark the file for deletion;

F4.2.10.2. ☐ mark the file for transfer;

F4.2.10.3. ☐ change the retention period (or assign a different schedule) so that the file is retained and re-reviewed at a later date. *(*Based on MoReq 5.2.5)

F4.2.11. ☐ The EDRMS should allow the reviewer to enter comments into the file's metadata to record the reasons for the review decisions. *(*Based on MoReq 5.2.6)

F4.2.12. ☐ The EDRMS should alert the Administrator to files due for disposal before implementing disposal actions; and on confirmation from the Administrator the EDRMS should be capable of initiating the disposal actions. *(*Based on MoReq 5.2.7)

F4.2.13. ☐ The EDRMS should store in the audit trail all decisions taken by the reviewer during reviews. *(*Based on MoReq 5.2.9)

F4.2.14. ☐ The EDRMS should provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process, by tracking:

F4.2.14.1. ☐ progress/status of the review, such as awaiting or in-progress, details of reviewer and date;

F4.2.14.2. ☐ records awaiting disposal as a result of a review decision;

F4.2.14.3. ☐ progress of the transfer process. *(*Based on MoReq 5.2.10)

F4.2.15. ☐ The EDRMS should be able to accumulate statistics of review decisions in a given period and provide tabular and graphical reports on the activity. *(*Based on MoReq 5.2.11)

F4.3. Disposition and Transfer/Export

Disposition refers to the destruction of records or the transfer of *the legal custody* (ownership) of the records to an agency external to government (i.e., their alienation from the Crown provincial) or to the BC Archives.

Transfer/export indicates transfer of physical records to off-site storage facilities and/or transfer or export of electronic records to external systems. For example, it may be necessary to export file/volumes to another EDRMS and it will be necessary to export transfer/export selected file/volumes of records to the BC Archives for permanent preservation.

Transfer/export will include both record content and descriptive material relating to record context, such as file structure, file/volume and record metadata. To support the process of review and preparation for transfer, it may be necessary to add free-text annotations as metadata at the file/volume level, such as: the primary/secondary classifications to be used

for records transferred to a new organisation; the reasons for transfer/disposition decisions; accession numbers or other data supplied by BC Archives for use in archival finding aids; etc.

Disposition

F4.3.1. ☐ The EDRMS should permit disposition to be processed for files covered by approved records schedules only (i.e., not for files linked to draft schedules).

F4.3.2. ☐ All volumes/records associated with a file should be disposed before the disposition of the file is confirmed by the EDRMS.

F4.3.3. ☐ The EDRMS should provide orderly processes supporting the application of a records schedule's disposition instructions, including processes for:

F4.3.3.1. ☐ review of the electronic file/volume and contents;

F4.3.3.2. ☐ export of the electronic file/volume and contents for permanent preservation;

F4.3.3.3. ☐ destruction of the electronic file/volume and contents. *(*Based on PRO, A.3.13)

F4.3.4. ☐ The EDRMS should require approval by a Records Officer or authorized delegate before permitting or performing destruction of any record.

F4.3.5. ☐ The EDRMS should allow individual and batch destruction action upon authorized approval and confirmation.

F4.3.6. ☐ The EDRMS should enable the total destruction of files and records that are stored on rewritable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities. *(*Based on MoReq 5.3.13)

F4.3.7. ☐ If records are stored on write-once media, the EDRMS should provide facilities to prevent access to them so that they cannot be restored by normal use of the EDRMS or by standard operating system utilities. *(*Based on MoReq 5.3.14)

F4.3.8. ☐ The EDRMS should support documentation of on-site records destruction of both electronic and physical records (i.e., destruction of records *not* stored in off-site storage facilities managed by BC Archives). This documentation should include lists of files/records eligible for destruction, reports documenting authorizations, and date of completed destruction.

Transfer/Export (e.g., to other EDRMS or to BC Archives)

F4.3.9. ☐ The EDRMS should provide a well-managed process to transfer records to another system or to a third party organization. *(*Based on MoReq 5.3.1)

F4.3.10. ☐ The EDRMS should be able to support the flagging of electronic files/volumes and groups of files/volumes for export to another EDRMS, or for transfer to the BC Archives for permanent preservation. *(*Based on PRO A.3.25)

F4.3.11. ☐ The EDRMS should be able to identify and list electronic files/volumes marked for permanent preservation as their disposal schedules come into force. *(*Based on PRO A.3.26)

F4.3.12. The EDRMS should provide the ability to:

F4.3.12.1. ☐ add user-defined metadata elements (e.g., elements required for archival management purposes) to electronic file/volumes selected for transfer;

F4.3.12.2. ☐ sort electronic files/volumes selected for transfer into ordered lists according to user-defined metadata elements;

F4.3.12.3. ☐ generate user-defined forms to describe electronic files/volumes that are being exported or transferred. *(*Based on MoReq 5.3.11; PRO A.3.42)

F4.3.13. ☐ Where an EDRMS does not support the addition of metadata to electronic files/volumes selected for export or transfer, and the sorting of files/volumes into ordered lists, it should interface with an appropriate package (for example a report management package) for this purpose. *(*Based on PRO A.3.29)

F4.3.14. ☐ The EDRMS should support transfer of electronic records to BC Archives in both native and non-proprietary formats (XML preferred).

F4.3.15. ☐ The EDRMS should ensure profile information is available for files transferred to the legal custody of the BC Archives is available in standard, non-proprietary format (XML preferred).

F4.3.16. ☐ The EDRMS should provide a utility or conversion tool to support the rendition of records marked for transfer or export into specified transfer format(s), e.g.:

F4.3.16.1. ☐ extensible mark-up language (XML);

F4.3.16.2. ☐ single page TIFF images (TIFF ver 6.0 with lossless compression;

F4.3.16.3. ☐ Delimited (e.g., Comma Separated Variable Length). (Based on MoReq 5.3.5)

F4.3.17. ☐ Where an EDRMS does not support the rendering of records and files/volumes marked for transfer into an approved transfer format, it should interface with an appropriate package or conversion utility for this purpose. *(*Based on PRO A.3.30)

F4.3.18. Whenever the EDRMS transfers the contents of any primary classification, file or volume, the transfer should include:

F4.3.18.1. ☐ all files in a primary class (for classes);

F4.3.18.2. ☐ all volumes below the file in the hierarchy (for files);

F4.3.18.3. ☐ all records in all these files and volumes;

F4.3.18.4. ☐ All metadata associated with the files, records and volumes. *(*Based on MoReq 5.3.2)

F4.3.19. ☐ The EDRMS should be able to export a whole electronic file or entire set of files within a primary classification in one sequence of operations, such that:

F4.3.19.1. ☐ the content and appearance of the electronic records are not degraded;

F4.3.19.2. ☐ all components of an electronic record, when the record consists of more than one component, are exported as an integral unit; for example, an e-mail message with associated file attachment;

F4.3.19.3. ☐ all metadata associated with an electronic record is linked to the record to which it belongs;

F4.3.19.4. ☐ all electronic records within a specific file/volume remain associated with that file/volume;

F4.3.19.5. ☐ all electronic file/volume metadata is exported and remains associated with that electronic file/volume. *(*Based on MoReq 5.3.3; PRO A.3.27)

F4.3.20. ☐ The EDRMS should be able to export groups of electronic files/volumes, or an entire primary of the classification scheme in one sequence of operations, such that all conditions of the above requirement are met, and:

F4.3.20.1. ☐ the relative location of each file/volume in the electronic file plan structure is maintained, so that the file/volume structure can be reconstructed;

F4.3.20.2. ☐ all file/volume metadata at higher points in the hierarchy is retained with that file/volume. *(*Based on MoReq 5.3.8; PRO A.3.40)

F4.3.21. ☐ Whenever the EDRMS transfers or exports records, the EDRMS must be able to include a copy of all the audit trail data associated with the files, volumes and records being transferred. *(*Based on MoReq 5.3.4)

F4.3.22. ☐ The EDRMS should be able to export multiple entries, where an electronic file/volume to be exported contains a pointer rather than the physical record; at a minimum, by achieving this effect through duplication of records to be exported. *(*Based on PRO A.3.28)

F4.3.23. ☐ The EDRMS should be able to export and transfer multiple entries (i.e., links between a physical record and its entry in more than one file/volume) without duplication of records. *(*Based on PRO A.3.39)

F4.3.24. ☐ The EDRMS should produce a report detailing any failure during a transfer, export or deletion. The report should identify any records destined for transfer which have generated processing errors, and any files or records and associated metadata which are not successfully transferred, exported or deleted. *(*Based on MoReq 5.3.6)

F4.3.25. ☐ The EDRMS should retain all electronic files that have been transferred, at least until confirmation of a successful transfer process. *(*Based on MoReq 5.3.7)

F4.3.26. ☐ Where hybrid files are to be transferred, exported or destroyed, the EDRMS should require the Administrator to confirm that the paper part of the same files has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part. *(*Based on MoReq 5.3.9)

F4.3.27. ☐ The EDRMS should allow records to be transferred or exported more than once. *(*Based on MoReq 5.3.17)

F4.3.28. ☐ The EDRMS should have the ability to retain metadata for files and records that have been destroyed or transferred. *(*Based on MoReq 5.3.15)

F4.3.29. ☐ The EDRMS should allow the Administrator to specify a subset of file metadata that will be retained for files destroyed, transferred out or moved offline, which can be indexed and retrieved alongside metadata for existing records, to indicate the absence of sought items. *(*Based on MoReq 5.3.16; PRO A.3.43)

F4.3.30. ☐ The EDRMS should support the selection and export of electronic record and file/volume metadata, independently from record content, in a form suitable for migration to a Web-based environment. *(*Based on PRO A.3.38)]

F5. Preservation and Ongoing Access

F5.1.1. ☐ The EDRMS should be capable of supporting the preservation of records beyond the anticipated life cycle of their source applications, by enabling the following preservation metadata to be captured in the records profiles:

F5.1.1.1. ☐ file names;

F5.1.1.2. ☐ hardware dependencies;

F5.1.1.3. ☐ operating system dependencies;

F5.1.1.4. ☐ application software dependencies (application names and versions);

F5.1.1.5. ☐ file formats;

F5.1.1.6. ☐ resolution;

F5.1.1.7. ☐ compression algorithm version and parameters;

F5.1.1.8. ☐ encoding scheme;

F5.1.1.9. ☐ rendition information. *(*Based on MoReq 12.7.13)

F5.1.2. ☐ The EDRMS should be able to retrieve records throughout their required retention periods by utilizing storage media with appropriate long-term life expectancy ratings and enabling the replacement of media, hardware, and software components to address component obsolescence. *(*Based on AIIM, p.8)

F5.1.3. ☐ The EDRMS should maintain internal integrity (relational integrity or otherwise) at all times, regardless of maintenance activities; other user actions; failure of system components. *(*Based on MoReq 3.4.12)

F5.1.4. ☐ The EDRMS should include features for the automated periodic comparison of copies of information, and the replacement of any copy found to be faulty, to guard against media degradation. *(*Based on MoReq 11.7.2)

F5.1.5. ☐ The EDRMS should allow the bulk conversion of records (with their metadata and audit trail information) to other media and/or systems in line with the standards relevant for the formats in use. *(*Based on MoReq 11.7.3)

F5.1.6. ☐ The EDRMS supplier should have a demonstrable program in place for upgrades to the EDRMS technology base that allows for the existing information to continue to be accessed without changes to the content. *(*Based on MoReq 11.7.4)

F5.1.7. ☐ The EDRMS should use only widely accepted standards that are the subject of open and publicly available specifications for encoding, storage and database structures. *(*Based on MoReq 11.7.5)

F5.1.8. ☐ If the EDRMS uses any proprietary encoding or storage or database structures, these should be fully documented, with the documentation being available to the Administrator. *(*Based on MoReq 11.7.6)

F6. Security

Security requirements include the ability to protect records from unauthorized destruction; define security categories for records; control user access to records and to system functions; maintain audit trails of system activities, and provide backup and recovery controls, including recovery of vital records.

F6.1. Deletion of Records

F6.1.1. ☐ The EDRMS should allow a default or option that prevents any record, once captured, from being deleted or moved by any Administrator or user. This means that any requirement for an Administrator to consider a record as "deleted" or "re-located" means that the record is marked appropriately; and in the case of re-location, a copy or pointer is inserted at the new location. *This requirement does not affect transfer or destruction of records in accordance with a retention schedule. (*Based on MoReq 9.3.1)

F6.1.2. ☐ The EDRMS should allow an option at configuration time, as an alternative to the deletion option specified above, that "deletion" of a record is implemented as destruction of that record. *(*Based on MoReq 9.3.2)

F6.1.3. If the EDRMS is configured so that "deletion" of a record is implemented as destruction of that record, the EDRMS should, in the event of any such deletion:

F6.1.3.1. ☐ record the deletion comprehensively in the audit trail;

F6.1.3.2. ☐ produce an exception report for the Administrator;

F6.1.3.3. ☐ delete the entire contents of a file or volume when it is deleted;

F6.1.3.4. ☐ ensure that no documents are deleted if their deletion would result in a change to another record (for example if a document forms a part of two records - one of which is being deleted);

F6.1.3.5. ☐ highlight to the Administrator any links from another file, or record to a file or volume that is about to be deleted, requesting confirmation before completing the deletion;

F6.1.3.6. ☐ maintain complete integrity of the metadata at all times. *(*Based on MoReq 9.3.7)

F6.2. Records Security Categories

F6.2.1. ☐ The Administrator should be able to change the security category of individual records. *(*Based on MoReq 9.3.3)

F6.2.2. ☐ The Administrator should be able to change the security category of all records in a file or class in one operation; the EDRMS should provide a warning if any records are having their security category lowered, and await confirmation before completing the operation. *(*Based on MoReq 9.3.4)

F6.2.3. ☐ The EDRMS should record full details of any change to security category in the metadata of the record, volume or file affected. *(*Based on MoReq 9.3.6

F6.2.4. ☐ The EDRMS should record the date on which a security classification should be reviewed. *(*Based on MoReq 12.5.19)

F6.2.5. ☐ Where files have security categories, the EDRMS should ensure that a hybrid physical file is allocated the same security category as an associated hybrid electronic file. *(*Based on MoReq 10.1.7)

F6.2.6. ☐ The EDRMS should include the ability to control access to records based on intellectual property restrictions, and generate charging data. *(*Based on MoReq 8.1.29)

F6.3. User Access/Authentication

F6.3.1. ☐ The EDRMS should integrate with security protocols, user authentication models and access control methods commonly deployed in similar government / industry environments; i.e., should:

F6.3.1.1. ☐ integrate with LDAP and Windows 2000 Active Directory;

F6.3.1.2. ☐ provide mechanisms to deal with document authentication, non-repudiation, integrity and privacy;

F6.3.1.3. ☐ provide methods to manage changing security policies.

F6.3.2. ☐ The EDRMS should integrate with common authentication services for access to existing and emerging document-related services. It should do this by:

F6.3.2.1. ☐ incorporating BC government security tables established through the BCGOV ID assigned to government employees and authorized personnel;

F6.3.2.2. ☐ provide a login that uses or is unified with that of the BC government LAN;

F6.3.2.3. ☐ allow users and groups to be imported from the operating system.

F6.3.3. ☐ The EDRMS should allow the Administrator to limit access to records, files and metadata to specified users or user groups. *(*Based on MoReq 4.1.1)

F6.3.4. ☐ The EDRMS should allow the Administrator to attach to the user profile attributes that determine the features, metadata fields, records or files to which the user has access. The attributes of the profile should:

F6.3.4.1. ☐ prohibit access to the EDRMS without an accepted authentication mechanism attributed to the user profile;

F6.3.4.2. ☐ restrict user access to specific files or records;

F6.3.4.3. ☐ restrict user access to specific parts of the classification scheme;

F6.3.4.4. ☐ restrict user access according to the user's security clearance;

F6.3.4.5. ☐ restrict user access to particular features (e.g., create, read, up-date and/or delete specific metadata fields; change records profile metadata, open/close files/volumes, register records, perform scheduling activities, dispose of physical and electronic records, etc);

F6.3.4.6. ☐ deny access after a specified date;

F6.3.4.7. ☐ allocate users to a group or groups. *(*Based on MoReq 4.1.2)

F6.3.5. ☐ The Administrator should be able to change any user-entered metadata element. Information about any such change should be stored in the audit trail

F6.3.6. ☐ The EDRMS should be able to provide the same control functions for roles as for users. *(*Based on MoReq 4.1.3)

This feature allows administrators to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Records Officer, Records Clerk, Database Administrator.

F6.3.7. ☐ The EDRMS should be able to set up groups of users that are associated with a set of files or records. *(*Based on MoReq 4.1.4)

Examples of groups might be Personnel, project working groups.

F6.3.8. ☐ The EDRMS should allow a user to be a member of more than one group. *(*Based on MoReq 4.1.5)

F6.3.9. ☐ The EDRMS should allow only Administrators to set up user profiles and allocate users to groups. *(*Based on MoReq 4.1.6)

F6.3.10. ☐ The EDRMS should allow a user to stipulate which other users or groups can access records for which the user is responsible. *(*Based on MoReq 4.1.7)

F6.3.11. ☐ The EDRMS should allow changes to security attributes for groups or users (such as access rights, security level, privileges, password allocation and management) to be made only by Administrators. *(*Based on MoReq 4.1.8)

F6.3.12. ☐ The EDRMS should support establishment of permissions that control scope of user searches (e.g., within specified organizational units; across specified organizational units; entire ministry).

F6.3.13. ☐ The EDRMS should not display record/volume/file information unless the user has access permissions for information. *(*Based on MoReq 8.1.28)

F6.3.14. If a user requests access to, or searches for, a record, volume or file which he or she does not have the right to access, the EDRMS should provide one of the following responses (selectable at configuration time):

F6.3.14.1. ☐ display title and metadata;

F6.3.14.2. ☐ display the existence of a file or record (i.e., display its file or record number) but not its title or other metadata;

F6.3.14.3. ☐ do not display any record information or indicate its existence in any way. *(*Based on MoReq 4.1.9)

F6.3.15. ☐ If a user performs a full text search, the EDRMS should never include in the search result list any record that the user does not have the right to access. *(*Based on MoReq 4.1.10)

F6.3.16. ☐ If the EDRMS allows users to make unauthorized attempts to access files, volumes or records, it should log these in the audit trail. *(*Based on MoReq 4.1.11)

It will be acceptable for this feature to be controllable so that it only applies to administrator-specified security categories.

F6.3.17. ☐ The EDRMS should provide the capability to limit users' access to parts of the file list (as specified at configuration time). *(*Based on MoReq 4.1.12)

F6.3.18. ☐ The EDRMS should include features to control and record access to physical files, including controls based on security category, which are comparable to the features for electronic files. *(*Based on MoReq 10.1.8)

F6.4. Audit

F6.4.1. The EDRMS should create an unalterable audit trail capable of automatically capturing and storing information about:

F6.4.1.1. ☐ all the actions that are taken upon an electronic record, electronic file or classification scheme;

F6.4.1.2. ☐ the user initiating and or carrying out the action;

F6.4.1.3. ☐ the date and time of the event. *(*Based on MoReq 4.2.1)

The word "unalterable" is to mean that the audit trail data cannot be modified in any way or deleted by any user; it may be subject to re-organisation and copying to removable media if required by, for example, database software, so long as its contents remains unchanged.

F6.4.2. ☐ Once the audit trail functionality has been activated, the EDRMS should track events without manual intervention, and store in the audit trail information about them. *(*Based on MoReq 4.2.2)

F6.4.3. ☐ The EDRMS should maintain the audit trail for as long as required, which will be at least for the life of the electronic records or electronic files to which it refers. *(*Based on MoReq 4.2.3)

F6.4.4. The EDRMS should provide an audit trail of all changes made to:

F6.4.4.1. ☐ groups of electronic files;

F6.4.4.2. ☐ individual electronic files;

F6.4.4.3. ☐ electronic volumes;

F6.4.4.4. ☐ electronic records;

F6.4.4.5. ☐ electronic documents;

F6.4.4.6. ☐ metadata associated with any of the above. *(*Based on MoReq 4.2.4)

F6.4.5. ☐ The EDRMS should provide an audit trail of all changes made to administrative parameters. *(*Based on MoReq 4.2.5)

For example, if the Administrator changes a user's access rights.

F6.4.6. The EDRMS should be capable of capturing and storing in the audit trail information about the following actions:

F6.4.6.1. ☐ the date and time of capture of all electronic records;

F6.4.6.2. ☐ re-classification of an electronic record in another electronic volume;

F6.4.6.3. ☐ re-classification of an electronic file within the classification scheme;

F6.4.6.4. ☐ any change to the retention schedule of an electronic file;

F6.4.6.5. ☐ any change made to any metadata associated with classes, electronic files or electronic records;

F6.4.6.6. ☐ date and time of creation, amendment and deletion of metadata;

F6.4.6.7. ☐ changes made to the access privileges affecting an electronic file, electronic record or user;

F6.4.6.8. ☐ export or transfer actions carried out on an electronic file;

F6.4.6.9. ☐ date and time of a rendition;

F6.4.6.10. ☐ deletion / destruction actions on an electronic file or electronic record. *(*Based on MoReq 4.2.6)

F6.4.7. ☐ The EDRMS should allow the audit trail facility to be configurable by the Administrator so that he can select the functions for which information is automatically stored; and the EDRMS should ensure that this selection and all changes to it are stored in the audit trail. *(*Based on MoReq 4.2.7)

F6.4.8. ☐ The EDRMS should ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorized external personnel who have little or no familiarity with the system. *(*Based on MoReq 4.2.8)

F6.4.9. ☐ The EDRMS should be able to export audit trails for specified electronic records, electronic files and groups of files (without affecting the audit trail stored by the EDRMS). *(*Based on MoReq 4.2.9)

F6.4.10. ☐ The EDRMS should be able to capture and store violations (i.e., a user's attempts to access a record, volume or file to which he or she is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms. *(*Based on MoReq 4.2.10)

F6.5. Backup and Recovery

F6.5.1. ☐ The EDRMS should provide automated backup and recovery procedures that allow for the regular backup of all or selected classification levels (e.g., primaries, secondaries), files, records, metadata and administrative attributes of the EDRMS repository. *(*Based on MoReq 4.3.1)

F6.5.2. The EDRMS should allow the Administrator to schedule backup routines by:

F6.5.2.1. ☐ specifying the frequency of backup;

F6.5.2.2. ☐ selecting classification levels (e.g., primaries, secondaries; files or records) to be backed up;

F6.5.2.3. ☐ selecting storage media, system or location for the backup (e.g., off-line storage, separate system, remote site). *(*Based on MoReq 4.3.2)

F6.6. Vital Records

F6.6.1. ☐ The EDRMS should allow users to indicate that selected records are considered to be "vital records". *(*Based on MoReq 4.3.6)

F6.6.2. ☐ The EDRMS should allow vital records and other records to be restored in distinct operations (e.g., it should be possible to recover vital records without having to achieve full recovery of all records in the same repository). *(*Based on MoReq 4.3.7)

F7. Printing and Reports

F7.1. Printing

F7.1.1. ☐ The EDRMS should provide the user with flexible ways of printing records and their relevant metadata, including the ability to print a record(s) with metadata specified by the user. *(*Based on MoReq 8.3.1).

F7.1.2. ☐ The EDRMS should allow the printing of metadata for a file. *(*Based on MoReq 8.3.2).

F7.1.3. ☐ The EDRMS should allow the user to be able to print out a summary list of selected records (e.g., the contents of a file), consisting of a user-specified subset of metadata elements (e.g., Title, Author, Creation date) for each record. *(*Based on MoReq 8.3.4).

F7.1.4. ☐ The EDRMS should allow the Administrator to specify that all printouts of records have selected metadata elements appended to them, e.g., title, registration number, date, security category. *(*Based on MoReq 8.3.5).

F7.1.5. ☐ The EDRMS should allow users to print search result hit lists. *(*Based on MoReq 8.3.6).

F7.1.6. ☐ The EDRMS should allow users to print search parameters.

F7.1.7. ☐ The EDRMS should allow the Administrator to print any and all administrative parameters. *(*Based on MoReq 8.3.7).

F7.1.8. ☐ The EDRMS should allow Administrators to print a thesaurus (e.g., schema of authorized/controlled indexing terms). *(*Based on MoReq 8.3.9)

F7.1.9. ☐ The EDRMS should allow Administrators to print file lists. *(*Based on MoReq 8.3.11)

F7.1.10. ☐ The EDRMS should allow Administrators to print audit trails. *(*Based on MoReq 8.3.12).

F7.1.11. ☐ The EDRMS should be able to print (at minimum) all common forms of BC government office records (e.g., MS Outlook and MS Office records). Printing should:

F7.1.11.1. ☐ preserve the layout produced by the generating application;

F7.1.11.2. ☐ include all (printable) components of the electronic record. *(*Based on MoReq 8.3.13)

F7.2. Reports

F7.2.1. The EDRMS should:

F7.2.1.1. ☐ provide "canned" (pre-defined) reports;

F7.2.1.2. ☐ support or link to an external application to support ad-hoc reports

F7.2.2. ☐ The EDRMS should provide the capability to produce/export reports in common and preferably non-proprietary electronic formats, including:

F7.2.2.1. ☐ XML;

F7.2.2.2. ☐ PDF.

F7.2.3. ☐ The EDRMS should support reports based on user criteria in order to perform location management functions to specified files/volumes, (i.e., inventories of holdings, box content file lists, audit reports, security reports, etc).

F7.2.4. ☐ The EDRMS should support eligibility reports (pull lists) based on user criteria to perform scheduling management actions, and organize reports as required by users. These reports should:

F7.2.4.1. ☐ identify missing or charged out files and/or volumes;

F7.2.4.2. ☐ note "holds" (or not bring up "holds") – all files should be eligible;

F7.2.4.3. ☐ arrange information in a way that facilitates the placement of volumes in boxes by final disposition date and final disposition type (like with like). The pull lists are based on profile data and classification data.

F7.2.5. ☐ The EDRMS should be able to produce standard box content file lists showing for each file/volume at minimum: the schedule, primary, secondary, file and volume numbers; primary, secondary and file titles/codes; OPR designation; and the earliest/latest record dates.

F7.2.6. ☐ The EDRMS should support management reports (statistics, usage, errors, etc) for records officer reporting.

F7.2.7. ☐ The EDRMS should support audit reports based on security parameters, use, access etc.

F7.2.8. ☐ The EDRMS should be able to produce a report listing of files and volumes, structured to reflect the classification scheme, for all or part of the classification scheme. *(*Based on MoReq 9.2.4)

F7.2.9. ☐ The EDRMS should include features for sorting and selecting report information. *(*Based on MoReq 9.2.5)

F7.2.10. ☐ The EDRMS should include features for totaling and summarizing report information. *(*Based on MoReq 9.2.6)

F7.2.11. ☐ The EDRMS should allow authorized users to request regular periodic reports and one-off reports. *(*Based on MoReq 9.2.7)

F7.3. Labelling

F7.3.1. ☐ EDRMS should be able to generate labels for the components of a file (e.g., file folders, filebacks, binders, tapes, and other physical containers for records).

F7.3.2. The EDRMS should support:

F7.3.2.1. ☐ the printing and recognition of bar codes; and/or

F7.3.2.2. ☐ other tracking systems (e.g., to automate the data entry for tracking physical box/file movements). *(*Based on MoReq 10.1.9)

F7.3.3. ☐ An authorized user (e.g. MRO) should be able to specify content of a label (fields that will print).

F7.3.4. ☐ A user should able to specify number of labels to print (single, multiple, or batch).

F7.3.5. ☐ A user should be able to generate different formats for file labels and volume labels

F8. Administrative Functions

F8.1. General Systems Administration

F8.1.1. ☐ The EDRMS should allow Administrators, in a controlled manner and without undue effort, to retrieve, display and re-configure systems parameters and choices made at configuration time–for example, on elements to be indexed–and to re-allocate users and functions to user roles. *(*Based on MoReq 9.1.1).

F8.1.2. ☐ The EDRMS should provide back-up facilities, and features to rebuild forward using restored back-ups and audit trails, while retaining system integrity. *(*Based on MoReq 9.1.2)

In other words, the EDRMS should include functionality to recreate the records and metadata to a known status, using a combination of restored back-ups and audit trails.

F8.1.3. ☐ The EDRMS should provide recovery and rollback facilities in the case of system failure or update error, and should notify Administrators of the results. *(*Based on MoReq 9.1.3)

In other words, the EDRMS should allow Administrators to "undo" a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

F8.1.4. ☐ The EDRMS should monitor available storage space, and notify Administrators when action is needed because available space is at a low level or because it needs other administrative attention. *(*Based on MoReq 9.1.4).

F8.1.5. ☐ The EDRMS should monitor error rates occurring on storage media, and report to the Administrator any medium or device on which the error rate is exceeding a parameter set at configuration time. *(*Based on MoReq 9.1.5)

This particularly applies to optical media.

F8.2. Administrative Reports

F8.2.1. ☐ The EDRMS should provide flexible reporting facilities for the Administrator. They should include, at a minimum, the ability to report the following items.

F8.2.1.1. ☐ numbers of files, volumes and records;

F8.2.1.2. ☐ transaction statistics for files, volumes and records;

F8.2.1.3. ☐ activity reports by user. (Based on MoReq 9.2.1)

F8.2.2. The EDRMS should allow Administrators to enquire on and produce reports on the audit trail. These reports should include, at a minimum, reporting based on items listed below:

F8.2.2.1. ☐ classification elements (primaries and secondaries);

F8.2.2.2. ☐ files;

F8.2.2.3. ☐ volumes;

F8.2.2.4. ☐ records;

F8.2.2.5. ☐ users;

F8.2.2.6. ☐ time periods. *(*Based on MoReq 9.2.2)

F8.2.3. The EDRMS should allow Administrators to enquire on and produce audit trail reports based on the items listed below:

F8.2.3.1. ☐ security categories;

F8.2.3.2. ☐ user groups;

F8.2.3.3. ☐ other metadata. *(*Based on MoReq 9.2.3)

F8.2.4. ☐ The EDRMS should allow Administrators to restrict users' access to selected reports. *(*Based on MoReq 9.2.8)

F9. Document Management

This section provides requirements for the document management portion of the Proponent's integrated EDRMS solution. The document management portion of the EDRMS should provide a robust enterprise infrastructure for building future document-centric business applications.

F9.1. General Requirements

F9.1.1. ☐ The document management portion of the EDRMS should fully support broadly available document services used to manage documents independent of the applications used to create them. These services should include the ability to:

- F9.1.1.1. ☐ check documents "in" and "out" of information repositories;
- F9.1.1.2. ☐ automatically update document version numbers whenever a previously "checked-out" document is modified and returned to the document repository;
- F9.1.1.3. ☐ prevent more than one person from checking documents out for modification;
- F9.1.1.4. ☐ utilize a security model ensuring that only authorized users can perform the above functions;
- F9.1.1.5. ☐ provide full lifecycle management capabilities for tracking of document versions /statuses;
- F9.1.1.6. ☐ provide full text searching capabilities in accordance with Common Command Language(CCL) (ISO 8777);
- F9.1.1.7. ☐ manage compound (virtual) documents. *(*Based on AIIM, pp. 13, 21)

F9.1.2. ☐ The document management portion of the EDRMS should support Enterprise Report Management (ERM) functionality. This is also known as Computer Output to Laser Disk (COLD) functionality.

F9.1.3. ☐ The document management portion EDRMS should provide the ability to manage annotations. In the case of CAD documents, this can be taken to mean the proposed system should provide the ability to manage redline mark ups as separate documents. These annotations should be controlled by a security mechanism that can control which users have access to annotations independently of any access controls documents to which they apply.

F9.1.4. ☐ The document management portion of the EDRMS should provide the ability to manage the components of a document. In the case of CAD documents, which often consist of "vector" components set against a "raster" background, all components of vector/raster hybrids should be associated for ease of search and retrieval.

F9.1.5. ☐ The document management portion of the EDRMS should provide the ability to automatically generate renditions of documents. This means that it should be possible for a document in one file format to have a rendition in another format associated with it.

The proposed system should be able to determine and dispatch the most appropriate rendition when a user requests a rendered document.

F9.1.6. ☐ The document management portion of the EDRMS should provide the ability to define (and redefine) document types and associated metadata. This functionality should be similar to, yet independent of, the profiling metadata of the records management portion of the EDRMS.

F9.1.7. The document management portion of the EDRMS should provide a security mechanism that has the following characteristics;

F9.1.7.1. ☐ security is set at the level of the document;

F9.1.7.2. ☐ security is managed through Access Control Lists (ACLs);

F9.1.7.3. ☐ document management security integrates with the records management security mechanisms.

F9.2. Interaction with RM Functions

Note: One intent of the following requirements is to ensure that future technology components brought into the integrated system will not defeat the records management functions of the EDRMS.

F9.2.1. ☐ The document system should be able to access the Records Management metadata, which should be protected from modifications through the document management system.

F9.2.2. ☐ The document management portion of the EDRMS should be able to capture automatically electronic documents arising in the course of business and pass them to the EDRMS records registration process. *(*Based on MoReq 10.3.1)

F9.2.3. ☐ The document management portion of the EDRMS should be able to capture an electronic record in one process OR register an electronic document that can be captured as a record at a later time. *(*Based on MoReq 10.3.2)

F9.2.4. ☐ The document management portion of the EDRMS should allow users to register a document from within the document management client software or an application integrated with the EDRMS, such as the applications of the Microsoft Office Suite. *(*Based on MoReq 10.3.3)

F9.2.5. ☐ When users are in the document management portion of the EDRMS or in an application integrated with the EDRMS, they should be able to switch adroitly to and from the records management portion of the EDRMS in order to register a document as a record. *(*Based on MoReq 10.3.4)

F9.2.6. ☐ The document management portion of the EDRMS should support automated acquisition of metadata elements and allow additional metadata elements to be completed by the user. *(*Based on MoReq 10.3.5)

F9.2.7. ☐ The document management portion of the EDRMS should be able to manage electronic documents (not registered as records) in the context of the same classification scheme and access control mechanisms as electronic records. *(*Based on MoReq 10.3.7)

F9.2.8. ☐ The document management portion of the EDRMS should be able to access the *ARCS/ORCS* classification system. *(*Based on MoReq 10.3.8)

F9.2.9. ☐ The document management portion of the Proponent's solution should have capabilities for managing versions of electronic documents as separate but related entities. It should provide capabilities for pruning unwanted versions and provide tools to automate the management of version histories. *(*Based on MoReq 10.3.9)

F9.2.10. ☐ The document management portion of the EDRMS should be configurable to restrict users to viewing either the latest version of a document, or selected versions of a document. or versions that have been captured as records. Access to this functionality should be in accordance with set security policies. *(*Based on MoReq 10.3.10)

F9.2.11. ☐ The document management portion of the EDRMS should be able to integrate with related software, including image processing and scanning systems, and workflow systems, without relinquishing control of any existing electronic records. *(*Based on MoReq 10.3.11)

F9.2.12. ☐ The document management portion of the EDRMS should be able to copy the content of an electronic record, in order to create a new electronic document, while ensuring the retention of the original record remains intact. *(*Based on MoReq 10.3.12)

F10. Other Functionality

F10.1. Workflow

F10.1.1. ☐ The document management portion of the EDRMS should provide or link to an engine for building ad hoc or collaborative workflows that meet the standards set out by the Workflow Management Coalition (WfMC) for document-centric workflows, including support for WfMC Application Programming Interfaces (API's).

F10.1.2. ☐ The EDRMS should provide or support the construction of workflows for records scheduling, review and export/transfer processes; e.g., by enabling the tracking of:

F10.1.2.1. ☐ progress of the review - awaiting, in progress, reviewer details and date;

F10.1.2.2. ☐ awaiting disposal as a result of a review decision;

F10.1.2.3. ☐ progress of records transfer processes.

F10.1.3. ☐ The EDRMS should support workflows consisting of a number of steps, each step being (for example) movement of a record or file from one participant to another for action. *(*Based on MoReq 10.4.1)

F10.1.4. ☐ The EDRMS should not practically limit the number of steps in each workflow. *(*Based on MoReq 10.4.2)

F10.1.5. ☐ The EDRMS should provide a function to alert a user participant that documents records have been sent for attention and specify the action required. *(*Based on MoReq 10.4.3)

F10.1.6. ☐ The EDRMS should enable a user to send e-mail messages to users to notify them of records requiring their attention. *(*Based on MoReq 10.4.4)

F10.1.7. ☐ The EDRMS should allow programmed workflows to be defined and maintained by the Administrator. *(*Based on MoReq 10.4.5)

F10.1.8. ☐ The EDRMS should prevent programmed workflows from being changed by users other than the Administrator, or by approved users authorized by the Administrator. *(*Based on MoReq 10.4.6)

F10.1.9. ☐ The EDRMS should allow Administrators to designate that individual users are able to reassign tasks/actions to different users or user groups. *(*Based on MoReq 10.4.7)

F10.1.10. ☐ The EDRMS should record all changes to programmed workflows in the audit trail. *(*Based on MoReq 10.4.8)

F10.1.11. ☐ The EDRMS should record the progress of a record or file through a workflow so that users can determine the status of a record or file in the process. *(*Based on MoReq 10.4.9)

F10.1.12. ☐ The EDRMS should not practically limit the number of workflows that can be defined. *(*Based on MoReq 10.4.10)

F10.1.13. ☐ The EDRMS should support management of files and records in queues that can be examined or controlled by the Administrator and authorized users. *(*Based on MoReq 10.4.11)

F10.1.14. ☐ The EDRMS should be capable of letting participants view queues of work addressed to them and select items to be worked on. *(*Based on MoReq 10.4.12)

F10.1.15. ☐ The EDRMS should provide conditional flows depending on user input or system data. *(*Based on MoReq 10.4.13)

F10.1.16. ☐ The EDRMS should provide a reminder, or bring-forward, facility for files and records. *(*Based on MoReq 10.4.14)

F10.1.17. ☐ The EDRMS should allow users to pause or interrupt a flow (i.e., to suspend it) temporarily in order to be able to attend to other work. *(*Based on MoReq 10.4.15)

F10.1.18. ☐ The EDRMS should recognize individuals and groups as participants in a workflow. *(*Based on MoReq 10.4.16)

F10.1.19. ☐ The EDRMS should provide a facility to “load balance” by distributing incoming items to group members in rotation or based on a set of business rules defined by the Administrator. *(*Based on MoReq 10.4.17)

F10.1.20. ☐ The EDRMS should provide an ability to prioritize items in queues. *(*Based on MoReq 10.4.18)

F10.1.21. ☐ The EDRMS solution should be able to associate time limits with individual steps and/or process in each flow, and report items that are overdue according to these limits. *(*Based on MoReq 10.4.20)

F10.1.22. ☐ The EDRMS should allow the receipt of electronic documents to trigger workflows automatically. *(*Based on MoReq 10.4.21)

F10.1.23. ☐ The EDRMS should provide reporting facilities to allow management to monitor workflow volumes, performance and exceptions. *(*Based on MoReq 10.4.22)

F10.1.24. ☐ The EDRMS workflow feature should prevent pre-programmed workflows from being changed by users other than the Administrator, or by approved users authorized by the Administrator. *(*Based on MoReq 10.4.6)

F10.2. Electronic Signatures

Note: It is assumed that a digital signature will need to be verified prior to entering the record, and the details of verification recorded once it has done so. It should not be necessary to routinely verify digitally signed records once they are registered, since they will be managed within the EDRMS in a manner that ensures authenticity.

F10.2.1. ☐ The EDRMS should be able to retain the information relating to electronic signatures, encryption and details of related verification agencies. *(*Based on MoReq 10.5.1)

F10.2.2. ☐ The EDRMS should have a structure, which permits the easy introduction of different electronic signature technologies. *(*Based on MoReq 10.5.2)

F10.2.3. ☐ The EDRMS should be able to retain and preserve as metadata, details about the process of verification for an electronic signature, including:

F10.2.3.1. ☐ the fact that the validity of the signature was checked;

F10.2.3.2. ☐ the Certification Authority with which the signature has been validated;

F10.2.3.3. ☐ the date and time that the checking occurred. *(*Based on MoReq 10.5.4)

F10.2.4. ☐ The EDRMS should be capable of checking the validity of an electronic signature at the time of capture of the record. *(*Based on MoReq 10.5.5)

F10.2.5. ☐ The EDRMS should include features which allow the integrity of records bearing electronic signatures to be maintained (and to prove it has been maintained), even though an Administrator has changed some of its metadata, but not the content of the record, after the electronic signature was applied to the record. *(*Based on MoReq 10.5.6)

F10.2.6. The EDRMS should be able to store with the electronic record:

F10.2.6.1. ☐ the electronic signature(s) associated with that record;

F10.2.6.2. ☐ the digital certificate(s) verifying the signature;

F10.2.6.3. ☐ any confirming counter-signatures appended by the certification authority in such a way that they are capable of being retrieved in conjunction with the record, and without prejudicing the integrity of a private key. *(*Based on MoReq 10.5.7)

F10.3. Encryption

F10.3.1. ☐ Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the EDRMS, the EDRMS should be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control allocated to that record. *(*Based on MoReq 10.6.1)

F10.3.2. Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the EDRMS, the EDRMS should be able to keep as metadata with that record:

F10.3.2.1. ☐ the fact of encrypted transmission;

F10.3.2.2. ☐ the type of algorithm;

F10.3.2.3. ☐ the level of encryption used. *(*Based on MoReq 10.6.2)

F10.3.3. ☐ The EDRMS should be able to ensure the capture of encrypted records directly from a software application which has an encrypting capability, and restrict access to those users listed as holding the relevant decryption key. *(*Based on MoReq 10.6.3)

F10.3.4. ☐ The EDRMS should allow encryption to be removed when a record is imported or captured. (Based on MoReq 10.6.4)

This feature may be desired in some large-scale record archives that have a requirement for long-term access (because encryption etc. is likely to reduce the ability to read records in the long term). In this case, the organisation would rely on audit trail or similar information to prove that the encryption etc. had been present but has been removed. In other environments, this feature may be undesirable from a legal point of view.

F10.3.5. ☐ The EDRMS should have a structure that permits different encryption technologies to be introduced easily. *(*Based on MoReq 10.6.5)

F10.4. Electronic Watermarks

F10.4.1. ☐ The EDRMS should be capable of storing records bearing electronic watermarks, and of storing with them information about the watermark. *(*Based on MoReq 10.7.1)

F10.4.2. ☐ The EDRMS should be able to retrieve information stored in electronic watermarks. *(*Based on MoReq 10.7.2)

F10.4.3. ☐ The EDRMS should have a structure that permits different watermarking technologies to be introduced easily. *(*Based on MoReq 10.7.3)

F11. General Requirements

F11.1. Ease of Use

F11.1.1. ☐ The EDRMS should enable users to access electronic document services from both client workstations and remotely connected computers; with:

F11.1.1.1. ☐ a full range of services delivered to desktop clients in a familiar windows environment;

F11.1.1.2. ☐ (at minimum) search, view and download services available to remote users.

F11.1.2. ☐ The EDRMS should fully support inter/intranet web based technology, where

F11.1.2.1. ☐ web servers provide all necessary mechanisms to store and retrieve information requested by users, system level security for users and data, and system management functions;

F11.1.2.2. ☐ web browsers provide a common user interface for accessing the EDRMS applications and document repositories.

F11.1.3. ☐ The EDRMS should provide the ability of users to enable users to save information in user-selectable formats. At minimum, these should include:

F11.1.3.1. ☐ HTML;

F11.1.3.2. ☐ XML;

F11.1.3.3. ☐ PDF.

F11.1.4. The EDRMS should support web publishing by providing:

F11.1.4.1. ☐ a mechanism for authorized users to create HTML and XML templates for specific classes or types of documents;

F11.1.4.2. ☐ convert documents to the above templates for web distribution.

F11.1.5. ☐ The EDRMS should provide online help throughout the EDRMS. *(*Based on MoReq 11.1.1)

F11.1.6. ☐ The online help in the EDRMS should be context-sensitive. *(*Based on MoReq 11.1.2)

F11.1.7. ☐ All error messages produced by the EDRMS should be meaningful, so that they can be appropriately acted upon by the users who are likely to see them. *(*Based on MoReq 11.1.3)

F11.1.8. ☐ The EDRMS should employ a single set of user interface rules, or a small number of sets. These should be consistent with the operating system environment in which the EDRMS operates. *(*Based on MoReq 11.1.4)

F11.1.9. ☐ The EDRMS should be able to display several records simultaneously. *(*Based on MoReq 11.1.5).

F11.1.10. ☐ Where the EDRMS uses on-screen windows, each should be user-configurable. *(*Based on MoReq 11.1.6)

F11.1.11. ☐ The EDRMS user interface should be suitable for users with special needs; that is, compatible with specialist software that may be used and with appropriate interface guidelines (e.g., W3C Web Content Accessibility Guideline, Microsoft Official Guidelines for User Interface Developers and Designers). *(*Based on MoReq 11.1.7)

F11.1.12. ☐ Where the EDRMS includes the use of windows, it should allow users to move, re-size and modify their appearance, and to save modifications in a user profile. *(*Based on MoReq 11.1.9)

F11.1.13. ☐ The EDRMS should allow users to select sound and volume of audio alerts, and to save modifications in a user profile. *(*Based on MoReq 11.1.10)

F11.1.14. ☐ The EDRMS should allow persistent defaults for data entry where desirable. These defaults should include:

F11.1.14.1. ☐ user-definable values;

F11.1.14.2. ☐ values same as previous item;

F11.1.14.3. ☐ values derived from context, e.g., date, file reference, user identifier; as appropriate. *(*Based on MoReq 11.1.11)

F11.1.15. ☐ The EDRMS should be closely integrated with MS Outlook in order to allow users to send electronic records and files electronically without leaving the EDRMS. *(*Based on MoReq 11.1.13)

F11.1.16. ☐ The EDRMS should provide integration with MS Outlook by sending pointers to files and records rather than copies, whenever a file or record is sent to another user of the EDRMS. *(*Based on MoReq 11.1.14)

F11.1.17. Where the EDRMS employs a graphical user interface, it should allow users to customize it. Customization should include, but need not be limited to the following changes:

F11.1.17.1. ☐ menu contents;

F11.1.17.2. ☐ layout of screens;

F11.1.17.3. ☐ use of function keys;

F11.1.17.4. ☐ on-screen colours, fonts and font sizes;

F11.1.17.5. ☐ audible alerts. (Based on MoReq 11.1.15)

F11.1.18. ☐ The EDRMS should support user-programmable functions. *(*Based on MoReq 11.1.16)

For example, user-definable macros.

F11.1.19. ☐ The EDRMS should provide the capability to perform global data updates.

F11.1.20. ☐ The EDRMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records. *(*Based on MoReq 11.1.17)

F11.1.21. ☐ Where users have to enter metadata from images of printed documents, the EDRMS should provide features to allow the use of optical character recognition to capture metadata from the image (zoned optical character recognition). *(*Based on MoReq 11.1.17)

F11.1.22. ☐ The EDRMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records. *(*Based on MoReq 11.1.18)

F11.2. Product Maturity and Currency

F11.2.1. ☐ The EDRMS should use mature components, with each component having a history of regular updates to provide: new functionality, 'bug' fixes, adherence to new standards

and technologies, and continued integration with standard office applications and with current/emerging document-related applications. Such maturity and currency should be demonstrable/verifiable for the EDRMS:

F11.2.1.1. ☐ document management component;

F11.2.1.2. ☐ records management component for electronic records;

F11.2.1.3. ☐ records management component for physical records. (Based on AIM, p. 20)

PROVIDE EVIDENCE OF THE ABILITY OF THE PROPOSED SOLUTION TO MEET THE PRODUCT MATURITY/CURRENCY REQUIREMENTS; E.G.:

- **IDENTIFY MAJOR NEW RELEASES/UPGRADES FOR EACH COMPONENT OVER THE PAST 2 YEARS**
- **IDENTIFY INTERFACES/INTEGRATION ACHIEVED OVER THE PAST 2 YEARS WITH RELATED APPLICATIONS/TECHNOLOGIES**

F11.3. Scalability

F11.3.1. ☐ The EDRMS should be fully scaleable and should:

F11.3.1.1. ☐ NOT have any features that would preclude use in small or large organizations, with varying numbers of differently sized organizational units. *(*Based on MoReq 11.2.8)

F11.3.1.2. ☐ allow for an increase of the number of users and volumes of data without replacing primary system components (i.e., scalability in terms of increased memory, disk storage, optical storage, CPU speed and size, etc.). (AIIM p. 19)

F11.3.1.3. ☐ NOT impose limits the on numbers of classification elements, files/volumes, or records. *(*Based on MoReq 3.2.9)

F11.3.1.4. ☐ The EDRMS applications should have a high degree of modularity, allowing for implementation of additional functionality without adversely affecting the overall system (i.e., ability to add routing, OCR, automated fax services, workload distribution, form management, etc.). *(*AIIM, p. 9)

F11.3.2. The EDRMS should meet the following criteria for enterprise-wide implementation within the context of the BC government:

F11.3.2.1. ☐ ability to deploy EDRMS application(s) to every employee desktop ;

F11.3.2.2. ☐ support for large numbers of users who could require access to a single document repository or to multiple repositories;

F11.3.2.3. ☐ support for a distributed environment where multiple repositories (databases, servers, optical jukeboxes, etc.) exist in multiple, widely dispersed geographic locations;

F11.3.2.4. ☐ support replication between repositories;

F11.3.2.5. ☐ integrate with a wide range of technologies to be found within the crown corporations and ministries of the BC government;

F11.3.2.6. ☐ provide tools for monitoring and tuning system performance.

F11.3.3. ☐ All components of the EDRMS solution should be equally scalable and robust.

ATTACH A DESCRIPTION OF THE ABILITY OF THE PROPOSED SOLUTION TO MEET THE SCALABILITY REQUIREMENTS; E.G.,

- **DESCRIPTIONS OF THE LARGEST INSTALLATION/TESTING DONE TO DATE, INCLUDING NUMBER AND TYPES OF SERVERS, NUMBER OF TOTAL USERS, NUMBER OF AVERAGE CONCURRENT USERS, NUMBER OF RECORDS STORED, DATA SIZE OF RECORDS STORED (IN TERABYTES), INDEX/METADATA SIZE (IN GIGA/TERABYTES), SEARCH RESPONSE TIME, FILE ACCESS TIME, ETC.**

F11.4. Performance

F11.4.1. ☐ The EDRMS should provide adequate response times for commonly performed functions under standard conditions;

F11.4.1.1. ☐ 75% of the total user population for a particular repository/organization logged on and active (potentially several thousand concurrent users);

F11.4.1.2. ☐ users performing a mix of system functions at various rates. *(*Based on MoReq 11.2.1)

F11.4.2. ☐ The EDRMS should be able to perform a simple search within 3 seconds and a complex search (combining four terms) within 10 seconds regardless of the storage capacity or number of files and records on the system. *(*Based on MoReq 11.2.2)

In this context, performing a search means returning a result list. It does not include retrieving the records themselves.

F11.4.3. ☐ The EDRMS should be able to retrieve and display within 4 seconds the first page of a record that has been accessed within the previous 3 months, regardless of storage capacity or number of files/records on the system. *(*Based on MoReq 11.2.3)

This requirement is intended to allow for rapid retrieval of frequently used records, on the understanding that frequency of use is typically correlated with recent use.

F11.4.4. ☐ The EDRMS should be able to retrieve and display within 20 seconds the first page of a record that has not been accessed within the previous 3 months, regardless of storage capacity or number of files/records on the system. . *(*Based on MoReq 11.2.4)

This requirement is intended to allow for cases where a form of hierarchical storage management is used, where records used infrequently are stored on slower media than more active records.

F11.4.5. ☐ It should be possible to expand the EDRMS, in a controlled manner, up to at least 30 thousand users while providing effective continuity of service. *(*Based on MoReq 11.2.6)

F11.4.6. ☐ The EDRMS should support the above scalability requirements, including routine maintenance of:

F11.4.6.1. ☐ user and group data;

F11.4.6.2. ☐ access profiles;

F11.4.6.3. ☐ classification schemes;

F11.4.6.4. ☐ databases;

F11.4.6.5. ☐ retention schedules;

in the face of the anticipated levels of organisational change, without imposing undue systems/account administration overheads. *(*Based on MoReq 11.2.7)

F11.5. Openness, Connectivity and Standards

F11.5.1. ☐ The EDRMS should utilize industry standard components (without proprietary architectures), commonly available throughout the document management, imaging and workflow industries. *(*Based on AIIM, p. 13)

F11.5.2. ☐ The EDRMS should use industry standard interfaces for any scanning interface proposed, e.g. TWIN and ISIS.

F11.5.3. ☐ The proponent should indicate which third party document scanning/conversion applications they support or have successfully integrated with.

F11.5.4. ☐ The proponent should indicate what/which storage systems are supported e.g. drives and raw access; via the file system and data files; or file system and native record objects.

F11.5.5. ☐ The document management portion of the EDRMS should meet recommended industry standards, including:

F11.5.5.1. ☐ adherence to the Association for Information and Image Management's (AIIM) Document Management Alliance Specification (DMA) for software component interoperability;

F11.5.5.2. ☐ adherence to the Open Document Management API (ODMA) specifications for application programming interfaces. *(*Based on AIIM, pp. 13, 19, 28)

F11.5.6. ☐ The document management portion of the EDRMS should provide a rich set of programming interfaces that will integrate with applications as the BC government brings them into use. The EDRMS should enable the users to write applications, either client-server or thin client that will operate on MS Windows desktops, in one or more languages such as:

F11.5.6.1. ☐ Java;

F11.5.6.2. ☐ Visual Basic;

F11.5.6.3. ☐ C++

F11.5.6.4. ☐ Proprietary scripting/development environment.

F11.5.7. ☐ The document management portion of the EDRMS should support or provide the ability to build web-based access to documents in the system. This requirement means that the proposed solution should be able to transfer/receive information, metadata and records to/from an Enterprise Portal application for inter/intranet access.

THE PROPONENT SHOULD INDICATE WHICH PORTAL SOFTWARE THE PROPOSED DOCUMENT MANAGEMENT SYSTEM HAS BEEN LINKED TO.

F11.5.8. ☐ The EDRMS should support the storage of records using file formats and encoding which are either de jure standards or which are fully documented. *(*Based on MoReq 11.4.4)

F11.5.9. ☐ The EDRMS should conform to the search and retrieval and information exchange standards, including ISO 23950, Information retrieval – application service definition and protocol specification (ANSI Z39.50). *(*Based on MoReq 11.4.5)

F11.5.10. ☐ Relational databases used by the EDRMS should conform to the SQL standard, ISO/IEC 9075, Information technology – database languages – SQL (Based on MoReq 11.4.6)

F11.5.11. ☐ The EDRMS should store all country names in a format compliant with ISO 3166, Codes for the representation of names of countries. *(*Based on MoReq 11.4.8)

F11.5.12. ☐ The EDRMS should store all language names in a format compliant with ISO 639, Codes for the representation of names of languages. *(*Based on MoReq 11.4.9)

F11.5.13. ☐ If the EDRMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 8859-1 encoding. *(*Based on MoReq 11.4.10)

F11.5.14. ☐ If the EDRMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 10646 encoding (Unicode). *(*Based on MoReq 11.4.11)

F12. Technical Requirements

F12.1. Ability to Operate within BC Government Technology Infrastructure

F12.1.1. ☐ The EDRMS should be capable of operating within the current BC government Technology Infrastructure as outlined in **Appendix I** of this RFP.

ATTACH AN EXPLANATION OF THE PROPOSED APPROACH FOR MEETING THE TECHNICAL REQUIREMENTS; E.G.:

- **ABILITY OF THE PROPOSED EDRMS APPLICATION TO MEET THE REQUIREMENT "OUT OF THE BOX";**
- **REQUIRED APPLICATION CUSTOMIZATION;**
- **OTHER RELEVANT CONSIDERATIONS, INCLUDING ANY PRACTICAL LIMITS ON THE SIZE OF THE ELETRONIC RECORD STORE (X TERABYTES/X MILLION RECORDS) AND NUMBER OF USERS ABLE TO CONCURRENTLY USE THE EDRMS OR A PARTICULAR REPOSITORY WITHIN THE EDRMS.**

Request for Proposals

All enquiries related to this Request for Proposals, including any requests for information and clarification, are to be submitted by **October 18, 2021** and directed, in writing, to **Bradley.Weaver@bcogc.ca,** who will respond if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Commission's option.

RFP 21222005

Electronic Document and Records Management Planning in Microsoft 365

Closing Time: Proposal must be received electronically **before 2:00 PM** Pacific Time on: **October 29, 2021**

Delivery of Proposals

Proposals must be submitted electronically.

To: https://procurement.bcogc.ca/

Organization Overview

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for overseeing oil and gas operations in British Columbia. Regulatory responsibility is delegated to the Commission through the *Oil and Gas* Activities *Act* and includes specified enactments under the *Forest Act, Heritage Conservation Act, Land Act, Environmental Management Act*, and *Water Act*. The operating costs of the Commission are funded through industry fees and levies on a cost recovery basis.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected by ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

The regulatory responsibility of the Commission extends from the exploration and development phases of oil and gas activities through to facilities operation, and ultimately decommissioning of industry projects. It is charged with balancing a broad range of environmental, economic and social considerations.

A. Definitions and Administrative Requirements

1. Definitions

Throughout this Request for Proposals, the following definitions apply:

a) "Contract" means the written agreement resulting from this Request for Proposals executed by the Commission and the Contractor;
b) "Contractor" means the successful Proponent to this Request for Proposals who enters into a written Contract with the Commission;
c) "Must", or "mandatory" means a requirement that must be met in order for a proposal to receive consideration;
d) "Proponent" means an individual or a company that submits, or intends to submit, a proposal in response to this Request for Proposals;
e) "Commission" means the Oil and Gas Commission;
f) "Request for Proposals" means the process described in this document; and
g) "Should" or "desirable" means a requirement having a significant degree of importance to the objectives of the Request for Proposals.

2. Terms and Conditions

Submitting a proposal indicates acceptance of all the terms and conditions set out in the RFP, including those that follow and that are included in all appendices and any Addenda.

A proposal must be signed by a person authorized to sign on behalf of the Proponent with the intent to bind the Proponent to the RFP and to the statements and representations in the Proponent's proposal. A scanned copy of the signed cover page of this RFP is acceptable as is a cover letter identifying the Proponent, identifying the RFP and including a signature of an authorized representative of the Proponent that confirms the Proponent's intent to be bound. For proposals submitted to an electronic proposal constitutes the signature of an authorized representative of the Proponent and is acceptable without additional signature.

3. Electronic Submissions

For electronic submissions the following applies:

a) The Proponent is solely responsible for ensuring that the complete electronic Proposal, is received before Closing Time;
b) The maximum size of each attachment must be 500 MB or less and uploaded in a single attachment;
c) Proponents should submit proposal submissions in a single upload and avoid sending multiple submissions for the same opportunity;
d) Attachments must not be compressed, must not contain a virus or malware, must not be corrupted and must be able to be opened. Proponents submitting by electronic submission are solely responsible for ensuring that any emails or attachments are not corrupted. The Commission may reject proposals that are compressed, cannot be opened or that contain viruses or malware or corrupted attachments.

4. Additional Information Regarding the Request for Proposals

All subsequent information regarding this Request for Proposals, including changes made to this document will be posted on the BC Bid website at www.bcbid.ca. It is the sole responsibility of the Proponent to check for amendments on the BC Bid website.

5. Late Proposals

Proposals will be marked with their receipt time once submitted. Only complete proposals received and marked before closing time will be considered to have been received on time. Proposals that are received late will be marked late and will not be considered or evaluated. In the event of a dispute, the proposal receipt time as recorded by the electronic date stamp shall prevail whether accurate or not.

6. Eligibility

a) Proposals will not be evaluated if the Proponent's current or past corporate or other interests may, in the Commission's opinion, give rise to a conflict of interest in connection with the project described in this Request for Proposals. This includes, but is not limited to, involvement by a Proponent in the preparation of this Request for Proposals. If a Proponent is in doubt as to whether there might be a conflict of interest, the Proponent should consult with the Commission Contract Management Analyst prior to submitting a proposal.
b) Proposals from not-for-profit agencies will be evaluated against the same criteria as those received from any other Proponents.

7. Evaluation

Evaluation of proposals will be by a committee formed by the Commission and may include employees and contractors of the Commission. All personnel will be bound by the same standards of confidentiality. The Commission's intent is to enter into a Contract with the Proponent who has the highest overall ranking.

8. Negotiation Delay

If a written Contract cannot be negotiated within thirty days of notification of the successful Proponent, the Commission may, at its sole discretion at any time thereafter, terminate negotiations with that Proponent and either negotiate a Contract with the next qualified Proponent or choose to terminate the Request for Proposals process and not enter into a Contract with any of the Proponents.

9. Debriefing

At the conclusion of the Request for Proposals process, all Proponents will be notified of the award by BCBid. Unsuccessful Proponents may request a debriefing meeting with the Commission.

10. Alternative Solutions

If alternative solutions are offered, please submit the information in the same format, as a separate proposal.

11. Changes to Proposals

By submission of a clear and detailed written notification, the Proponent may amend or withdraw its proposal prior to the closing date and time. Upon closing time, all proposals become irrevocable. The Proponent will not change the wording of its proposal after closing and no words or comments will be added to the proposal unless requested by the Commission for purposes of clarification.

12. Proponents' Expenses

Proponents are solely responsible for their own expenses in preparing a proposal and for subsequent negotiations with the Commission, if any. If the Commission elects to reject all proposals, the Commission will not be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the proposal, loss of anticipated profit in connection with any final Contract, or any other matter whatsoever.

c)

13. Limitation of Damages

Further to the preceding paragraph, the Proponent, by submitting a proposal, agrees that it will not claim damages, for whatever reason, relating to the Contract or in respect of the competitive process, in excess of an amount equivalent to the reasonable costs incurred by the Proponent in preparing its proposal and the Proponent, by submitting a proposal, waives any claim for loss of profits if no Contract is made with the Proponent.

14. Proposal Validity

Proposals will be open for acceptance for at least 90 days after the closing date.

15. Firm Pricing

Prices will be firm for the entire Contract period unless this Request for Proposals specifically states otherwise.

16. Currency and Taxes

Prices quoted are to be:

a) In Canadian dollars;
b) Inclusive of duty, where applicable; FOB destination, delivery charges included where applicable; and
c) Exclusive of taxes

17. Completeness of Proposal

By submission of a proposal the Proponent warrants that, if this Request for Proposals is to design, create or provide a system or manage a program, all components required to operate the system or manage the program have been identified in the proposal or will be provided by the Contractor at no charge.

18. Subcontracting

a) Using a subcontractor (who should be clearly identified in the proposal) is acceptable. This includes a joint submission by two Proponents having no formal corporate links. However, in this case, one of these Proponents must be prepared to take overall responsibility for successful performance of the Contract and this should be clearly defined in the proposal.
b) Subcontracting to any firm or individual whose current or past corporate or other interests may, in the Commission's judgment, give rise to a conflict of interest in connection with the project or program described in this Request for Proposals will not be tolerated. This includes, but is not limited to, any firm or individual involved in the formulation of this Request for Proposals. If a Proponent is in doubt as to whether a proposed subcontractor gives rise to a conflict of interest, the Proponent should consult with the Commission Contact Person listed on page 1 prior to submitting a proposal.
c) Where applicable, the names of approved sub-contractors listed in the proposal will be included in the Contract. No additional subcontractors will be added, nor other changes made, to this list in the Contract without the written consent of the Commission.

19. Acceptance of Proposals

a) This Request for Proposals should not be construed as an agreement to purchase goods or services. The Commission is not bound to enter into a Contract with the Proponent who submits the lowest priced proposal or with any Proponent. Proposals will be assessed in light of the evaluation criteria. The Commission will be under no obligation to receive further information, whether written or oral, from any Proponent.

b) Neither acceptance of a proposal nor execution of a Contract will constitute approval of any activity or development contemplated in any proposal that requires any approval, permit or license pursuant to any federal, provincial, regional district or municipal statute, regulation or by-law.

20. Definition of Contract

Notice in writing to a Proponent that it has been identified as the successful Proponent and the subsequent full execution of a written Contract will constitute a Contract for the goods or services, and no Proponent will acquire any legal or equitable rights or privileges relative to the goods or services until the occurrence of both such events.

21. Contract

By submission of a proposal, the Proponent agrees that should its proposal be successful, the Proponent will enter into a Contract with the Commission in accordance with the terms of the Commission's General Service Agreement.

22. Liability for Errors

While the Commission has used considerable efforts to ensure the information in this Request for Proposals is accurate, the information contained in this Request for Proposals is supplied solely as a guideline for Proponents. The information is not guaranteed or warranted to be accurate by the Commission, nor is it necessarily comprehensive or exhaustive. Nothing in this Request for Proposals is intended to relieve Proponents from forming their own opinions and conclusions with respect to the matters addressed in this Request for Proposals.

23. Modification of Terms

The Commission reserves the right to modify the terms of this Request for Proposals at any time in its sole discretion. This includes the right to cancel this Request for Proposals at any time prior to entering into a Contract with the successful Proponent.

24. Ownership of Proposals

All proposals submitted to the Commission become the property of the Commission. They will be received and held in confidence by the Commission, subject to the provisions of the *Freedom of Information and Protection of Privacy Act* and this Request for Proposals.

25. Use of Request for Proposals

Any part of this document, or any information provided by the Commission in relation to this Request for Proposals may not be used or disclosed, for any purpose other than for the submission of proposals. Without limiting the generality of the foregoing, by submission of a proposal, the Proponent agrees to hold in confidence all information provided by the Commission in relation to this Request for Proposals.

26. Reciprocity

The Commission may consider and evaluate any proposals from other jurisdictions on the same basis that the Commission purchasing authorities in those jurisdictions would treat a similar proposal from a British Columbia supplier.

27. No Lobbying

Proponents must not attempt to convey directly or indirectly with any employee, contractor or representative of the Commission, including the evaluation committee and any elected officials of the Commission, or with members of the public or the media, about the project described in this Request for Proposals or otherwise in respect of the Request for Proposals, other than as expressly directed or permitted by the Commission.

1. Summary of the Requirement

The BC Oil and Gas Commission (Commission) is seeking an interested party to create a management framework for unstructured electronic information, encompassing necessary analysis, planning and recommendations for the configuration of Microsoft 365 (M365) as a corporate recordkeeping system. The goal is to effectively manage the end-to-end life cycle of official Commission records in accordance with provincial legislation, policies and standards for government recordkeeping, in the places where staff collaborate and create records.

Secondary to this, the Commission requires an assessment of any functional gaps that may exist between M365 and the Commission's system requirements for Electronic Document and Records Management (EDRM) and provincial requirements.

This work will provide the Commission with a clearly defined framework and methodology for a "total" records management solution available to all employees.

2. Anticipated Schedule

The following table outlines the anticipated schedule for this RFP. All times identified in the table are in Pacific Time.

Event	Anticipated Date
Enquiries deadline	October 18, 2021
Request closing time	October 29, 2021, before 2:00PM PST
Interviews and reference checks as required	November 1-5, 2021
Preferred Proponent selected by	November 8, 2021
Commencement of work	November 2021

3. Commission Situation/Overview

The Commission is the provincial regulatory agency for permitting and overseeing oil and gas activities, from exploration and development through to operations and ultimately decommissioning of oil and gas industry projects under British Columbia jurisdiction. The Commission's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2020/21 - 2022/23 Service Plan available on the Commission's website at www.bcogc.ca.

3.1 Commission Responsibility

Oil and Gas Activities Act (OGAA):

The purposes of the Commission, outlined in Section 4 of the Oil and Gas Activities Act, are briefly summarized as follows:

(a) to regulate oil and gas activities in British Columbia in a manner that
  (i) provides for the sound development of the oil and gas sector, by fostering a healthy environment, a sound economy and social well-being,
  (ii) conserves petroleum and natural gas resources,
  (iii) ensures safe and efficient practices, and
  (iv) assists owners of petroleum and natural gas resources to participate equitably in the production of shared pools of petroleum and natural gas;

(b) to provide for effective and efficient processes for the review of applications for permits and to ensure that applications that are approved are in the public interest having regard to environmental, economic and social effects;

(c) to encourage the participation of First Nations and aboriginal peoples in processes affecting them;

(d) to participate in planning processes;

(e) to undertake programs of education and communication in order to advance safe and efficient practices and the other purposes of the commission.

Information Management Act (IMA):

The Commission is subject to the provisions of the Information Management Act (IMA), government's primary information management law. Compliance with the IMA requires the head of a government body to ensure that an appropriate system is in place for creating and maintaining government information that is an adequate record of that government body's decisions.

Section 19 of the IMA defines the responsibility of the head, as follows:

Responsibility of head of government body

19 (1) The head of a government body is responsible for ensuring that an appropriate system is in place within the government body for managing and securing government information.

(1.1) Without limiting subsection (1), the head of a government body is responsible for ensuring that an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines issued under section 6 (1) *[directives and guidelines]*, government information that is an adequate record of that government body's decisions.

(2) The head of a government body must take reasonable steps to ensure that the government body

(a) complies with directives issued under section 6 (1), and

(b) is guided by guidelines issued under that section.

(3) [Repealed 2017-7-5.]

(4) The head of a government body must take reasonable steps to ensure that the government body complies with the following:

(a) [Not in force.]

(b) section 10 *[when information schedule applies]*;

(c) section 13 *[information must be digitized before archiving]*.

(5) Despite subsection (4) (b), the head of a government body must ensure that no government information held by the government body is disposed of, except in accordance with an information schedule or an approval by the chief records officer under section 11 (1) (b) *[when no information schedule applies]*.

3.2 Commission Overview

The BC Oil and Gas Commission (Commission) has a complex array of information with long term value to the province, and a continuously evolving business and regulatory environment. As a government body, the Commission is required to manage its records using the government standard for classification, retention and disposition, including the *Administrative Records Classification System* (ARCS), the Commission's *Operational Records Classification System* (ORCS) and other approved records schedules. An integrated software solution is necessary to meet this responsibility and effectively manage Commission information, regardless of media, from creation to final disposition.

3.2.1 Background

The Records and Information Services and Information Systems and Technology branches have initiated a multi-phased approach to achieving a state of EDRM readiness.

Phase One: Information Schedule Redesign: The first phase, initiated in 2017, included modernization of the Commission's outdated Operational Records Classification System (ORCS), with the objective of:

- Achieving media neutrality (to ensure official records can exist in any format);
- Addressing functional gaps within the classification system (to ensure all records are covered); and
- Reviewing record retention periods for appropriateness (to ensure records are being retained long enough to meet business and legal requirements).

This schedule amendment was approved by the Chief Records Officer and is being implemented through the shared drive classification project (see below). A second amendment is underway to cover new functional program areas and create a data retention plan for structured data in systems. This is considered a long-term project.

Phase Two: Classification of unstructured records on shared drives. This work commenced in 2019, and includes de-duplication, addressing long file paths, permission review, organization and classification of electronic records on shared drives in accordance with the Commission's ORCS, ARCS, and other applicable schedules. A program-by-program approach is being taken. This work is ongoing and recognized as a long-term initiative.

Phase Three: EDRM Needs Assessment. Completed in the spring of 2021, the Commission engaged an external consulting company to evaluate Commission EDRM requirements, based on the BC government EDRMS Request for Proposal (RFP). The final report outlined high level Commission EDRM system criteria (refer to *Appendix A: EDRM Business Requirements Summary*).

3.2.2 Current Situation

The Commission is migrating to Microsoft Office 365 (M365) and Azure for enterprise usage and intends to use existing M365 information governance functionality to manage unstructured digital records (both content created within M365 and currently residing on shared drives). While current licensing is E3, the Commission is intending to purchase additional E5 licensing in fall of 2021.

Unstructured records in the Commission exist in various locations:

- Multiple Shared Drives
- Outlook
- Teams
- OneDrive

Teams Sites have been created for departments and projects and continue to be established on a case-by-case basis. SharePoint sites have been provided for specific purposes. A key driver of this project is the need to determine the best approach to embed RM foundations in SharePoint as it is rolled out across the Commission and provide necessary RM foundations in the entire M365 environment.

4. Budget/Schedule

Funding to support this project in fiscal year 2021/2022 is $30,000. Proponents are encouraged to provide their best, realistic estimate for the work that they propose to meet the Commission's requirements. The Commission welcomes innovative proposals that reduce costs or duration, or that provide added value.

Preferred timeline for completion of contract deliverables is by **February 28, 2022,** or sooner, if possible.

5. Requirements

5.1 Scope of Services

The successful Proponent who enters into a written contract with the Commission is expected to provide the following services:

1. Delivery of a design for end-to-end records management within M365, including, but not limited to the labelling of content as a record (e.g., retention labels), retention requirements, specific deletion settings, specific permissions for records management functions, etc.
2. Recommendations and a detailed plan for configuring M365 as a recordkeeping system that addresses Commission requirements within the BC legislative and policy framework.
3. Analysis of any gaps between M365 functionality and Commission EDRM requirements.
4. Consultation, communications, and demonstrations with appropriate stakeholders.
5. Project schedule, and reporting – Proponent resources must be able to define project timelines, support meetings and/or reporting at the discretion of the Commission including regular status reports to inform on progress, risks, issues, spend to date, etc.
6. Presentation of findings to Commission Executive, if required.
7. Project closure – Proponent resources to be available to participate in project close out activities as required.

All deliverables will require the approval of the Commission before being accepted.

The Commission's Records and Information Services Branch will serve as the primary project contact. The Branch Director, and Specialist, EDRMS & Information Management Solutions will act as the product owners and work directly with the proponent as agreed to by both parties. Key members of the Information Systems Branch will be involved to provide necessary oversight, technical information and help facilitate contract deliverables.

5.2 Scope of Work

5.2.1 Understand Commission framework and environment

The selected Proponent will be able to demonstrate an understanding of the Commission's environment and how to ensure compliance with applicable legislation, policies, and best practices. This will include:

- Reviewing relevant documentation such as records classification and retention requirements, Commission M365 interim policies, and the EDRM Needs Assessment report.
- Understanding the current state of the unstructured data environment.
- Discussing project objectives, including high level goals and desired outcomes.

5.2.2 Develop a configuration plan that, at a minimum:

- Identifies the best approach/strategy for the Commission environment.
- Focuses on managing unstructured information within the M365 environment.
- Ensures a framework that supports collaboration.
- Provides configuration guidance for policies and retention labels and how they will be applied.
- Focuses on best practices and the user experience.
- Considers future migration of unstructured information into M365 through configuration.
- Addresses baseline metadata.
- Explore options for email classification and retention.

5.2.3 Document any gaps between Commission EDRM requirements and M365.

5.3 Deliverables

Project deliverables will include:

- A customized plan for an approach and methodology to configure M365 as a recordkeeping system. It will include practical guidance and instruction.
- Documented assessment and identification of any EDRM functional gaps that could impact the Commission's ability to comply with applicable legislation and policy.
- A project schedule.
- Status reports (format to be approved by Commission).
- Monthly invoicing including detailed hours worked.
- Executive presentation, if required.

5.4 Format Requirements

The following format, sequence, and instructions must be followed to provide consistency in Proponent response and ensure each proposal receives full consideration. With all pages consecutively numbered, the proposals should contain the following parts:

a) Table of contents with page numbers.

b) Executive summary.

c) The body of the proposal in accordance with the content requirements.

5.5 Content Requirements

Responses should be succinct and should focus on specific services and deliverables being proposed – please be considerate of the time it will take to review the submission.

To expedite a fair and unbiased proposal review process, the Commission's preference is for all proposals to use the following outline:

a) Project Approach (description the proposed approach, based on the scope described in section 5.2)

b) Costs/Schedule (including hourly rates, overall timelines, and total cost) provided in Canadian dollars (CAD).

c) Overall timeline

d) Budget breakdown

e) One example of **relevant** previous work

f) Resumes (max half page each)

6. Evaluation of Proponent Response

The evaluation of responses will be conducted by a team consisting of employees and/or contractors of the Commission. All members of the team will be bound by the same standards of confidentiality.

This section details all the mandatory and desirable criteria against which proposals will be evaluated. Proponents should ensure that they fully respond to all criteria to receive full consideration during the evaluation.

The lowest price or any Proposal will not necessarily be accepted. The Commission reserves the right to refuse any proposed based on quality, service, price, reputation, experience, and other criteria.

The Preferred Proponent will be the Proponent scoring the most points after evaluation. The evaluation process will consist of the following stages:

- Stage One – Mandatory Criteria
- Stage Two – Desirable Criteria
- Stage Three – Informational Interviews (optional and not scored)

6.1 Mandatory Criteria

Proposals not clearly demonstrating that they meet the following mandatory criteria will be excluded from further consideration during the evaluation process:

- **The Proposal must be received before the designated closing date and time.**
- **The Proposal must be in English.**
- **The Proponent must confirm that any personal information received, collected or held over the course of the review will be stored and used only in Canada.**
- **The Proposal must contain an independence and objectivity statement confirming the Proponent is free of any actual or perceived conflict of interest and free of bias with respect to the Commission, its officers, and employees.**

Failure to meet all mandatory criteria above will disqualify the Proponent's Proposal from further review.

6.2 Desirable Criteria

The Commission seeks to enter into an agreement with the Proponent who, in the opinion of the Commission, has the resources, knowledge and competence to provide the greatest value. Proposals meeting all the mandatory criteria will be further assessed against desirable criteria.

Desirable Criteria	Weight
Proponent's Qualifications and Relevant Experience • Proposal demonstrates Proponent's advanced understanding of records management principles and EDRM functionality. • Proposal demonstrates Proponent's advanced knowledge of M365's Records Management / Information Governance functionality.	40%
Suitability of Proposed Approach • Proposal provides a clearly defined plan to address project requirements.	40%
Pricing • Total price, hourly rates	20%

6.3 Informational Interviews

The top ranking (to a maximum of three) Proponents may be asked to attend an interview with the evaluation team. During the interview, the evaluation committee may clarify and/or verify statements made in the written Response.

The requirement for interviews is optional. The Commission reserves the right to complete the evaluation process without Proponent interviews.

7. Appendices

7.1 *Appendix A: EDRM Business Requirements Summary*

Electronic Document and Records Management
Business Requirements Summary
October 2021

Electronic Document and Records Management (EDRM) Business Requirements Summary

Table of Contents

STATEMENT OF CONFIDENTIALITY 3
1. INTRODUCTION 4
1.1 PURPOSE 4
1.2 BACKGROUND 4
2. CURRENT PROCESS 4
SYSTEM SCOPE 4
2.1 BUSINESS AND TECHNICAL OBJECTIVES 4
2.2 SCOPE 4
2.3 RISKS AND ISSUES 5
2.4 CONSTRAINTS 5
3. REQUIREMENTS 6
3.1 FUNCTIONAL REQUIREMENTS 6
3.2 NON - FUNCTIONAL REQUIREMENTS 10
3.2.1 AUDIT LOGS 10
3.2.2 SECURITY CONTROLS 10
3.2.3 INPUT DATA VALIDATIONS 10
3.2.4 WEB INTERFACE DESIGN REQUIREMENTS 11
3.2.5 CONFIDENTIAL DATA REQUIREMENTS 11

Statement of Confidentiality

The recipient of this document agrees that the information contained herein is confidential and shall remain the sole and exclusive property of the BC Oil and Gas Commission (Commission). Disclosure of this information by the Commission to the recipient shall not be construed as granting or conferring, by license or otherwise, any rights in or to the confidential information.

The recipient of this document further agrees that the confidential information obtained from this document shall be held in strict confidence, to be used exclusively for the purpose intended by the Commission and shall not be imparted by the recipient to others.

1. Introduction

1.1 Purpose

The primary purpose of this document is to set the requirements for the Commission to appropriately manage its electronic records. These requirements will create a benchmark which can be used to evaluate the acquisition and implementation of an Electronic Document and Records Management (EDRM) system or solution that offers an integrated records management and document management tool set. As a result of this initiative, all employees will have the ability to manage and search electronic and physical (hard copy) documents and records in a consistent manner from their desktops or via a web browser. While not a "requirement", the overarching principle is that the Commission will prioritize user experience (i.e., user-friendliness), specifically the ability to embed EDRMS functionality into user processes as seamlessly as possible.

1.2 Background

The Commission wishes to significantly improve its capability to manage the electronic documents and records in its possession. A key objective is to establish an infrastructure for effectively managing all Commission records in a consistent, logical manner, from creation to final disposition, using a common set of tools, standards, and policies.

2 Current Process

Processes and/or workflows being addressed by the EDRM system include:

- Maintenance of the Operational Records Classification System (ORCS) and Administrative Records Classification System (ARCS) classification and retention schedules;
- Application of ORCS and ARCS retention schedules to Commission electronic and hard copy information;
- Replacement of networked shared drives for managing electronic business and program records; and
- Replacement of excel spreadsheets and hard copy file lists for tracking and searching offsite hard copy collections.

System Scope

2.1 Business and Technical Objectives

The key objective of this specification is to provide an EDRM system capable of controlling the creation, use and final disposition of electronic and hard copy records across the Commission. The EDRM must be able to schedule records using the Commission's standard system for classification, retention and disposition, including the Administrative Records Classification System (ARCS), Operational Records Classification Systems (ORCS) and other approved records schedules.

2.2 Scope

The scope of the project is the management of records stored within networked shared drives and the offsite records holdings tracked within spreadsheets and file lists.

2.3 Risks and Issues

Resources & Funding

Additional resources for FTEs and well as application and development costs may be prohibitive depending on the variances identified with existing or planned technology solutions.

Education & Training

Management of change is a risk by altering how users access and manage their information. Moving information from one form of data structure and technology application to another raises the risk that some of the information content or context will be lost therefore hindering the ability to find and work with the information. Therefore, elements such as education, training and communication must be managed as part of the overall migration to EDRM.

File Plan

Context is often provided by the position of the information in the file plan or filing structure. This can help the user understand what business purpose the information serves. Information can become unusable without this additional context. A lower-level folder titled simply with a date, for instance, tells the user very little about its contents. To maintain the context of the information in the form of its location in the original file plan or organization structure, there is a need to ensure that this contextual folder structure can be migrated alongside the content or hold this information in a metadata field or new file naming standard.

Metadata

There is a risk that the default system generated metadata will be altered upon migration to the EDRM system. Last modified date and author are two examples of metadata that may become critical pieces of metadata that will require consideration based on the records collections.

Embedded Objects and Links

There is a risk that by migrating documents to an EDRMS, embedded objects and links between documents and attachments could be lost. There is no standard way of exporting this information, which is usually created and managed internally in a way that is not designed for import into another system. Examples include spreadsheets linked to other spreadsheets within another network folder, between a document and associated charts or graphics, links to external websites and databases and directory shortcuts.

Security Classifications and Permissions

Appropriate security controls must be assigned to prevent risk of breaches of confidentiality or disclosure of sensitive information.

2.4 Constraints

Capacity to retroactively align legacy IT system are limited although future systems will be developed to ensure compliance with Commission records governance requirements.

3 Requirements

Requirements have been grouped into sections based on their business objectives. Each section contains well-defined requirements and priorities.

Legend

Legend provides details on how individual requirements are defined in this document.

Req ID	*Requirements identification number*
Title	*Requirement title*
Project Priority	*Priority of each individual requirement [Mandatory, Desirable]*

3.1 Functional Requirements

The requirements address the business objectives gathered from the BCOGC.

Req ID:	*1.0*	**Title:**	*Basic Requirements*	**Project Priority**
1.01 Fully integrated document and records management functions for electronic and hard copy records available on desktops and web browsers.				Mandatory
1.02 Support management of records including but not limited to MS Office, Outlook, images, voicemail, desktop publishing, graphics, facsimiles, scanned documents, voice files, video files, digital schematics and maps.				Mandatory
1.03 Enable the authenticity, integrity, stability, and accessibility of electronic records over time, across systems and across formats.				Mandatory
1.04 Maintain standard metadata about electronic documents and files.				Mandatory
1.05 Maintain audit trails of actions taken on records.				Mandatory
1.06 Maintain the classification systems, i.e. enter new classifications, flag classifications as draft, and change to approved, change a retention that is already applied to a record, office of primary responsibility (OPR/NON-OPR) tags, etc.				Mandatory

Req ID:	*2.0*	**Title:**	*Identifying and Documenting Records*	**Project Priority**
2.01 Records must be classified in accordance with the established ORCS/ARCS classification systems.				Mandatory
2.02 When classified, the appropriate retention schedule must be applied.				Mandatory
2.03 Support the determination of the office of primary responsibility (OPR).				Mandatory
2.04 Allow for inheritance of records classification through parent and child relationships of folders or document containers.				Mandatory
2.05 Support the management of hybrid files containing both hard copy and electronic components in an integrated manner.				Mandatory
2.06 Support confidential data elements for protection of classes or sub-sets of records for public release.				Mandatory
2.07 Capture all the volumes relating to a file.				Mandatory
2.08 Allow for profile information to be amended or corrected.				Mandatory
2.09 Allow for creation of cross-references or 'see also' type of links between related files.				Mandatory

Req ID:	3.0	Title:	Metadata	Project Priority
3.01 Establish mandatory profile metadata for records including: unique identifiers, classification codes, file name, create date, modified date, date range of records, author.				Mandatory
3.02 Support specific sets of metadata elements for different types of electronic records i.e. UWI for well files.				Mandatory
3.03 Support specific sets of metadata elements for physical folders i.e. location for physical records, first and last dates for a physical volume, box number, accession numbers for off-site transfers.				Mandatory
3.04 Support multiple formats for metadata including free form text, alphanumeric, numeric, dates, logical (y/n, true/false).				Mandatory
3.05 Support inherited metadata elements.				Mandatory

Req ID:	4.0	Title:	Document Management	Project Priority
4.01 Support the checking in, locking or checking out of documents for editing by multiple users.				Mandatory
4.02 Support version control - allowing the user to determine whether minor or major versions are to be captured.				Mandatory
4.03 Issue a warning if a user attempts to save a document that has already been saved in the same file.				Mandatory

Req ID:	5.0	Title:	Preservation of Records	Project Priority
5.01 Records must be maintained on media and in formats that ensure they are readable and accessible for the duration of their active and semi-active retention periods.				Mandatory
5.02 Records scheduled for full or selective retention must be maintained on stable media appropriate for permanent retention.				Mandatory
5.03 The record format or media must be stable and not compromise the Commission's responsibilities or ability to use the information.				Mandatory
5.04 Document formats supported should be extendable as new formats are introduced.				Desirable
5.05 Profile information must be linked to records in a way that ensures they are identifiable and authentic, and the context of their creation and use is maintained.				Mandatory
5.06 Records moved to different media or electronic records moved to another custodian must maintain their context and authenticity.				Mandatory

Req ID:	6.0	Title:	Retention Scheduling	Project Priority
6.01 Support retention periods based on time (calendar year, fiscal year, trigger events or event / time retentions).				Mandatory
6.02 Designate active status at the file level and apply to all volumes.				Mandatory
6.03 Allow authorized users to change disposition assigned to a file at any time during its entire lifecycle.				Mandatory
6.04 Change file status when the active retention period elapses or when a defined trigger event occurs.				Mandatory
6.05 Provide 'scheduling date' to be set at the end of the scheduled active retention period - used to calculate when the file is eligible for final disposition.				Mandatory

	6.06 The date of the last record of a file may or may not be the same as the date on which the file's active retention period elapses.	Desirable
	6.07 A file with a semi-active retention period of "nil" (i.e., there is no semi-active retention period) moves to the end of its active and semi-active status at the same time.	Desirable

	Req ID:	*7.0*	**Title:**	*Transferring Records*	**Project Priority**
	7.01 New location of a file or volume must be captured.				Mandatory
	7.02 Volumes of one file may be transferred together or individually.				Mandatory
	7.03 Accession information must be captured for physical off-site storage facilities.				Mandatory

	Req ID:	*8.0*	**Title:**	*Final Disposition*	**Project Priority**
	8.01 Support final disposition types such as Destruction, Full Retention, Selective Retention or Other Disposition.				Mandatory
	8.02 Calculate retention periods and eligible disposition dates from 'scheduling date'.				Mandatory
	8.03 Permit authorized users to suspend retention periods and final disposition by applying a Hold that affects all components of a file or classes of files and permit them to lift a Hold.				Mandatory
	8.04 Authorize final disposition by designated individual(s).				Mandatory
	8.05 Apply final disposition to the entire container when files are stored in boxes or containers.				Mandatory
	8.06 Calculate disposition date for box based on file with the longest retention.				Desirable
	8.07 Permit destruction of electronic files so that they cannot be restored by use of a data recovery facility.				Mandatory
	8.08 Support batch destruction or transfer upon authorized approval and confirmation.				Mandatory
	8.09 Export whole electronic files without degradation, with metadata and associated file volumes.				Mandatory
	8.10 Retain all electronic files until confirmation of successful transfer.				Desirable
	8.11 Retain selected metadata for files destroyed or transferred.				Mandatory

	Req ID:	*9.0*	**Title:**	*Redaction*	**Project Priority**
	9.01 Prompt the creator of a redacted document to assign it to a file and store a cross reference to the original, potentially the same file or volume as the original record - even if record is closed.				Desirable

	Req ID:	*10.0*	**Title:**	*Workflow*	**Project Priority**
	10.01 Support the scheduling, review and transfer process by tracking progress of review, records awaiting disposal, records awaiting transfer.				Mandatory
	10.02 Support records scheduling disposition including review of records due for destruction, export of electronic files for permanent preservation and destruction of electronic file contents.				Mandatory
	10.03 Initiate the disposal notification workflow to named users as specified once retention period has been reached and allow them to mark the file for deletion, transfer or change the retention period and record comments.				Mandatory

	10.04 Support the construction of workflows for ad-hoc processes by authorized individuals.	Mandatory

	Req ID:	11.0	Title:	Reporting	Project Priority
	Ability to produce reports on multiple, user defined parameters including, but not limited to the following: • File contents, both hard copy and electronic with or without attributes • Classification and retention schedules • Files to which a specified retention schedule is assigned • Files to which a specified classification is assigned • Files to which a specified OPR is assigned • All files eligible for transfer or disposition • Frequency of retention period report, information reported and exceptions such as disposals overdue • Documents and all links for which it is a destination. • Records destruction of both electronic and physical records • Records marked for permanent preservation, export or transfer • Search parameters and results • Term stores or metadata values • Audit trails • Box content lists • Records designated for File Holds • Management reports of statistics, usage, etc.				Mandatory

	Req ID:	12.0	Title:	Searching	Project Priority
	12.01 Allow searching by classification codes, enterprise wide or 'from here', metadata, full text searching.				Mandatory
	12.02 Include searching of electronic and hard copy collections.				Mandatory
	12.03 Allow searching for free-text, Boolean, wild card, proximity, saved searches, refine searches, time intervals, full text.				Mandatory
	12.04 Display or save the search results.				Mandatory
	12.05 Do not display search results if the User does not have permission to see or access results.				Mandatory

	Req ID:	13.0	Title:	Migration and Bulk Loading	Project Priority
	13.01 Provide capability for authorized users to bulk load pre-existing hard copy file and volume records, electronic records and pre-determined metadata values.				Mandatory
	13.02 Support the rendition of records marked for transfer or export in XML, TIFF or CSV formats.				Mandatory
	13.03 Allow bulk conversion of records (with their metadata and audit trail information) to other media or systems in line with the standards relevant for the formats in use.				Mandatory

3.2 Non - Functional Requirements

The requirements may originate from leveraging the Commission's hardware and software. Requirements may also address the technical and business objectives gathered from the Commission.

3.2.1 Audit Logs

These requirements will be specific to ensuring that systems can be monitored.

Req ID:	*AL 1.0*	Title:	*Auditing Logs*	Project Priority
AL 1.01 Ability to monitor system including: • Authorized Access (UserID, Date/Time, Event Type, Resource Access) • Privileged Operations (Admin accounts access, System start/stop) • Failed access alerts (logon, data access)				Mandatory
AL 1.02 Retain audit trail information for as long as required				Mandatory

3.2.2 Security Controls

These requirements will be specific to ensuring that system/data access is restricted as required, and define authentication approach.

Req ID:	*SC 1.0*	Title:	*Security Controls*	Project Priority
SC 1.01 Restrict access in the system to authorized users.				Mandatory
SC 1.02 Allow for predetermined security policies assigned to records categories.				Mandatory
SC 1.03 Access restrictions based on security group membership (functionality and data.)				Mandatory
SC 1.04 Allow users to grant access to other users or groups to allow access to records for which they are responsible.				Mandatory
SC 1.05 Do not allow a user to view or include search results for which the user does not have rights to access.				Mandatory
SC 1.06 Integration with authentication methods for access to EDRM.				Mandatory
SC 1.08 New database security groups.				Mandatory
SC 1.09 Must support authentication with M365.				Mandatory
SC 1.10 Must use SSL for all traffic.				Mandatory

3.2.3 Input Data Validations

Req ID:	*ID 1.0*	Title:	*Input Data Validations*	Project Priority
ID 1.01 These requirements will be specific to ensuring that the quality and validity of the data input into the system is enforced, for example: • Limit field to specific data ranges • Define data types • Identify if field is mandatory or non mandatory • Identify if NULL value acceptable • Where applicable, define a finite list of acceptable values				Desirable

	• Verify plausibility of value where possible • Ensure key data cannot be overwritten or edited unless required – if required, audit functionality requirements should be gathered	

3.2.4 Web Interface Design Requirements

These requirements will define standard look and feel for application interfaces (not all will always apply), for example:

	Req ID:	*WI 1.0*	Title:	*Web Interface*	Project Priority
	WI 1.01 Must display the Commission (BCOGC) logo in the header				Desirable
	WI 1.02 Must provide link to BCOGC main website in footer				Desirable
	WI 1.03 Must display BCOGC Copyright in footer				Desirable
	WI 1.04 Must use BCOGC color scheme of olivedrab (#679147), midnightblue (#00456a) and white (#ffffff)				Desirable
	WI 1.05 Must support HTML5 compatible browsers				Desirable
	WI 1.06 Must scale to support mobile-friendly browsers				Desirable

3.2.5 Confidential Data Requirements

If the system manages or presents any 'confidential data', requirements must be defined to confirm they are managed appropriately.

	Req ID:	*CD 1.0*	Title:	*Confidential Data*	Project Priority
	CD 1.01 Ensure confidential data (security) requirements limit access to those who should be able to view this data; or need to ensure no confidential data requirements are presented. i.e. Payroll, HR, personnel records, third party landowner information.				Mandatory

Request for Proposals

All enquiries related to this Request for Proposals, including any requests for information and clarification, are to be submitted by **November 26, 2021** and directed, in writing, to **procurement@bcogc.ca,** who will respond if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Commission's option.

RFP # 21422003

Modern Digital Workplace

Closing Time: Proposal must be received electronically **before 2:00 PM** Pacific Time on: **December 3, 2021**

Delivery of Proposals

Proposals must be submitted electronically.

To: https://procurement.bcogc.ca/

Proponent's Meeting

A Proponent's meeting will not be held.

Organization Overview

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for overseeing oil and gas operations in British Columbia. Regulatory responsibility is delegated to the Commission through the *Oil and Gas* Activities *Act* and includes specified enactments under the *Forest Act, Heritage Conservation Act, Land Act, Environmental Management Act*, and *Water Sustainability Act*. The operating costs of the Commission are funded through industry fees and levies on a cost recovery basis.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected by ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

The regulatory responsibility of the Commission extends from the exploration and development phases of oil and gas activities through to facilities operation, and ultimately decommissioning of industry projects. It is charged with balancing a broad range of environmental, economic and social considerations.

A. Definitions and Administrative Requirements

1. Definitions

Throughout this Request for Proposals, the following definitions apply:

a) "Contract" means the written agreement resulting from this Request for Proposals executed by the Commission and the Contractor;
b) "Contractor" means the successful Proponent to this Request for Proposals who enters into a written Contract with the Commission;
c) "Must", or "mandatory" means a requirement that must be met in order for a proposal to receive consideration;
d) "Proponent" means an individual or a company that submits, or intends to submit, a proposal in response to this Request for Proposals;
e) "Commission" means the Oil and Gas Commission;
f) "Request for Proposals" means the process described in this document; and
g) "Should" or "desirable" means a requirement having a significant degree of importance to the objectives of the Request for Proposals.

2. Terms and Conditions

Submitting a proposal indicates acceptance of all the terms and conditions set out in the RFP, including those that follow and that are included in all appendices and any Addenda.

A proposal must be signed by a person authorized to sign on behalf of the Proponent with the intent to bind the Proponent to the RFP and to the statements and representations in the Proponent's proposal. A scanned copy of the signed cover page of this RFP is acceptable as is a cover letter identifying the Proponent, identifying the RFP and including a signature of an authorized representative of the Proponent that confirms the Proponent's intent to be bound. For proposals submitted to an electronic proposal constitutes the signature of an authorized representative of the Proponent and is acceptable without additional signature.

3. **Electronic Submissions**

For electronic submissions the following applies:

a) The Proponent is solely responsible for ensuring that the complete electronic Proposal, is received before Closing Time;
b) The maximum size of each attachment must be 500 MB or less and uploaded in a single attachment;
c) Proponents should submit proposal submissions in a single upload and avoid sending multiple submissions for the same opportunity;
d) Attachments must not be compressed, must not contain a virus or malware, must not be corrupted and must be able to be opened. Proponents submitting by electronic submission are solely responsible for ensuring that any emails or attachments are not corrupted. The Commission may reject proposals that are compressed, cannot be opened or that contain viruses or malware or corrupted attachments.

4. Additional Information Regarding the Request for Proposals

All subsequent information regarding this Request for Proposals, including changes made to this document will be posted on the BC Bid website at www.bcbid.ca. It is the sole responsibility of the Proponent to check for amendments on the BC Bid website.

5. Late Proposals

Proposals will be marked with their receipt time once submit. Only complete proposals received and marked before closing time will be considered to have been received on time. Proposals that are received late will be marked late and will not be considered or evaluated. In the event of a dispute, the proposal receipt time as recorded by the electronic date stamp shall prevail whether accurate or not.

6. **Eligibility**

a) Proposals will not be evaluated if the Proponent's current or past corporate or other interests may, in the Commission's opinion, give rise to a conflict of interest in connection with the project described in this Request for Proposals. This includes, but is not limited to, involvement by a Proponent in the preparation of this Request for Proposals. If a Proponent is in doubt as to whether there might be a conflict of interest, the Proponent should consult with the Commission Procurement Specialist prior to submitting a proposal.
b) Proposals from not-for-profit agencies will be evaluated against the same criteria as those received from any other Proponents.

7. Evaluation

Evaluation of proposals will be by a committee formed by the Commission and may include employees and contractors of the Commission. All personnel will be bound by the same standards of confidentiality. The Commission's intent is to enter into a Contract with the Proponent who has the highest overall ranking.

8. Negotiation Delay

If a written Contract cannot be negotiated within thirty days of notification of the successful Proponent, the Commission may, at its sole discretion at any time thereafter, terminate negotiations with that Proponent and either negotiate a Contract with the next qualified Proponent or choose to terminate the Request for Proposals process and not enter into a Contract with any of the Proponents.

9. Debriefing

At the conclusion of the Request for Proposals process, all Proponents will be notified of the award by BCBid. Unsuccessful Proponents may request a debriefing meeting with the Commission.

10. Alternative Solutions

If alternative solutions are offered, please submit the information in the same format, as a separate proposal.

11. Changes to Proposals

By submission of a clear and detailed written notification, the Proponent may amend or withdraw its proposal prior to the closing date and time. Upon closing time, all proposals become irrevocable. The Proponent will not change the wording of its proposal after closing and no words or comments will be added to the proposal unless requested by the Commission for purposes of clarification.

12. Proponents' Expenses

Proponents are solely responsible for their own expenses in preparing a proposal and for subsequent negotiations with the Commission, if any. If the Commission elects to reject all proposals, the Commission will not be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the proposal, loss of anticipated profit in connection with any final Contract, or any other matter whatsoever.

13. Limitation of Damages

Further to the preceding paragraph, the Proponent, by submitting a proposal, agrees that it will not claim damages, for whatever reason, relating to the Contract or in respect of the competitive process, in excess of an amount equivalent to the reasonable costs incurred by the Proponent in preparing its proposal and the Proponent, by submitting a proposal, waives any claim for loss of profits if no Contract is made with the Proponent.

14. Proposal Validity
Proposals will be open for acceptance for at least 90 days after the closing date.

15. Firm Pricing
Prices will be firm for the entire Contract period unless this Request for Proposals specifically states otherwise.

16. Currency and Taxes
Prices quoted are to be:
a) In Canadian dollars;
b) Inclusive of duty, where applicable; FOB destination, delivery charges included where applicable; and
c) Exclusive of taxes

17. Completeness of Proposal
By submission of a proposal the Proponent warrants that, if this Request for Proposals is to design, create or provide a system or manage a program, all components required to operate the system or manage the program have been identified in the proposal or will be provided by the Contractor at no charge.

18. Subcontracting
a) Using a subcontractor (who should be clearly identified in the proposal) is acceptable. This includes a joint submission by two Proponents having no formal corporate links. However, in this case, one of these Proponents must be prepared to take overall responsibility for successful performance of the Contract and this should be clearly defined in the proposal.
b) Subcontracting to any firm or individual whose current or past corporate or other interests may, in the Commission's judgment, give rise to a conflict of interest in connection with the project or program described in this Request for Proposals will not be tolerated. This includes, but is not limited to, any firm or individual involved in the formulation of this Request for Proposals. If a Proponent is in doubt as to whether a proposed subcontractor gives rise to a conflict of interest, the Proponent should consult with the Commission Contact Person listed on page 1 prior to submitting a proposal.
c) Where applicable, the names of approved sub-contractors listed in the proposal will be included in the Contract. No additional subcontractors will be added, nor other changes made, to this list in the Contract without the written consent of the Commission.

19. Acceptance of Proposals
a) This Request for Proposals should not be construed as an agreement to purchase goods or services. The Commission is not bound to enter into a Contract with the Proponent who submits the lowest priced proposal or with any Proponent. Proposals will be assessed in light of the evaluation criteria. The Commission will be under no obligation to receive further information, whether written or oral, from any Proponent.
b) Neither acceptance of a proposal nor execution of a Contract will constitute approval of any activity or development contemplated in any proposal that requires any approval, permit or license pursuant to any federal, provincial, regional district or municipal statute, regulation or by-law.

20. Definition of Contract
Notice in writing to a Proponent that it has been identified as the successful Proponent and the subsequent full execution of a written Contract will constitute a Contract for the goods or services, and no Proponent will acquire any legal or equitable rights or privileges relative to the goods or services until the occurrence of both such events.

21. Contract
By submission of a proposal, the Proponent agrees that should its proposal be successful, the Proponent will enter into a Contract with the Commission in accordance with the terms of the Commission's General Service Agreement.

22. Liability for Errors
While the Commission has used considerable efforts to ensure the information in this Request for Proposals is accurate, the information contained in this Request for Proposals is supplied solely as a guideline for Proponents. The information is not guaranteed or warranted to be accurate by the Commission, nor is it necessarily comprehensive or exhaustive. Nothing in this Request for Proposals is intended to relieve Proponents from forming their own opinions and conclusions with respect to the matters addressed in this Request for Proposals.

23. Modification of Terms
The Commission reserves the right to modify the terms of this Request for Proposals at any time in its sole discretion. This includes the right to cancel this Request for Proposals at any time prior to entering into a Contract with the successful Proponent.

24. Ownership of Proposals
All proposals submitted to the Commission become the property of the Commission. They will be received and held in confidence by the Commission, subject to the provisions of the *Freedom of Information and Protection of Privacy Act* and this Request for Proposals.

25. Use of Request for Proposals
Any part of this document, or any information provided by the Commission in relation to this Request for Proposals may not be used or disclosed, for any purpose other than for the submission of proposals. Without limiting the generality of the foregoing, by submission of a proposal, the Proponent agrees to hold in confidence all information provided by the Commission in relation to this Request for Proposals.

26. Reciprocity
The Commission may consider and evaluate any proposals from other jurisdictions on the same basis that the Commission purchasing authorities in those jurisdictions would treat a similar proposal from a British Columbia supplier.

27. No Lobbying
Proponents must not attempt to convey directly or indirectly with any employee, contractor or representative of the Commission, including the evaluation committee and any elected officials of the Commission, or with members of the public or the media, about the project described in this Request for Proposals or otherwise in respect of the Request for Proposals, other than as expressly directed or permitted by the Commission.

B. Requirements and Responses

1. Summary of the Requirement

The Commission is seeking interested parties to architect and develop a high availability, collaborative and integrated digital workplace built on the M365 platform. The Commission is licensed at an E5 level. Certain foundational elements of M365 have already been implemented and this project is aimed at extending the capabilities to address collaboration, knowledge sharing, improved search, and digital socialization aspects of a modern workplace. The Commission is also seeking support in establishing and participating in a sustainable governance model, as well as establishing and implementing a user centric adoption plan.

2. Anticipated Schedule

The following table outlines the anticipated schedule for this RFP. All times identified in the table are in Pacific Time.

Event	Anticipated Date
Enquiries deadline	November 26, 2021
Request closing time	December 3, 2021
Interviews and reference checks, as required	December 6-10, 2021
Preferred Proponent selected by	December 13, 2021
Commencement of work	January 2022

3. Commission Situation/Overview

The Commission is the provincial regulatory agency for permitting and overseeing oil and gas activities, from exploration and development through to operations and ultimately decommissioning of oil and gas industry projects under British Columbia jurisdiction. The Commission's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2021/22 – 2023/24 Service Plan available on the Commission's website at www.bcogc.ca.

3.1 Commission Responsibility

The purposes of the Commission, outlined in Section 4 of the Oil and Gas Activities Act, are briefly summarized as follows:

(a) to regulate oil and gas activities in British Columbia in a manner that
  (i) provides for the sound development of the oil and gas sector, by fostering a healthy environment, a sound economy and social well-being,
  (ii) conserves petroleum and natural gas resources,
  (iii) ensures safe and efficient practices, and
  (iv) assists owners of petroleum and natural gas resources to participate equitably in the production of shared pools of petroleum and natural gas;

(b) to provide for effective and efficient processes for the review of applications for permits and to ensure that applications that are approved are in the public interest having regard to environmental, economic and social effects;

(c) to encourage the participation of First Nations and aboriginal peoples in processes affecting them;

(d) to participate in planning processes;

(e) to undertake programs of education and communication in order to advance safe and efficient practices and the other purposes of the commission.

3.2 Background

The Commission's current intranet, MyOGC, was created in 2012, with a "refresh" in navigation in 2014. It is built on Drupal as a traditional intranet site and is nearing end-of life. It has been a significant internal communication tool for Commission news and updates to staff, but it has more recently been repurposed to meet new needs with non-optimal results. By modern standards, MyOGC is outdated in appearance, navigation, search, functionality, ease of use, and ease of administration.

In 2020, the Commission entered into an enterprise agreement with Microsoft for M365 services. This agreement entitles the Commission to use several Microsoft products including their online cloud services. M365 provides the Commission with an opportunity to modernize its workplace and advance its enterprise maturity. The Commission has already implemented some M365 foundational elements and services to enable a collaborative and remote work force. The Commission has already implemented the following M365 services to date:

- Identity Management
  - Azure Active Directory with multi-factor authentication
- Office 365 Suite of apps and client software (Word, Excel, PowerPoint, One Note)
- Exchange Online / Outlook
- Microsoft Teams (including Team sites)
- Security and Threat Detection (Azure ATP, Azure Sentinel)

To expand on the M365 foundations and seek a replacement for MyOGC, the Commission undertook a study to evaluate M365 services to use as an intranet replacement. The resulting recommendations were to take a holistic approach to M365 and using the platform as the next step in the evolution of the Commission's digital workplace.

3.3 Expected Project Outcomes

This initiative will be deemed successful when the following outcomes are realized. Based on staff interviews conducted during M365 evaluation, and in alignment with the Commission's Digital Workplace Program, this initiative aims to accomplish the following outcomes:

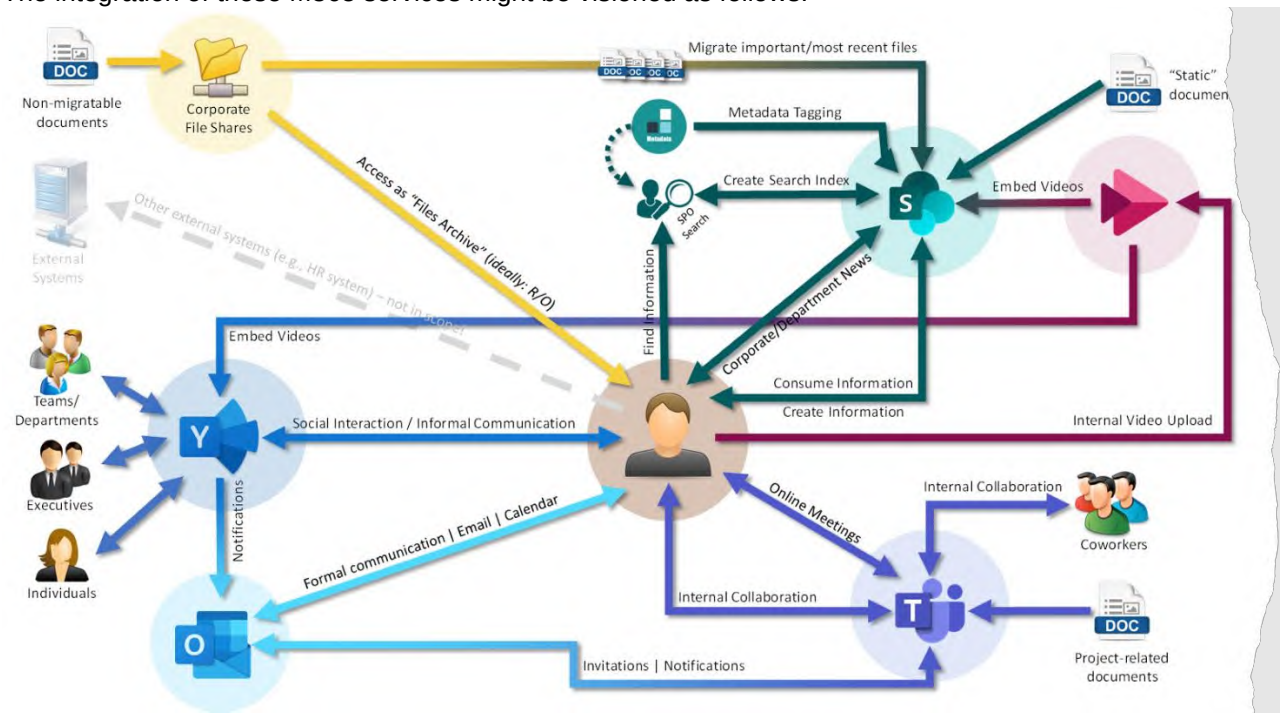
- Implement workplace tools that are user friendly and intuitive
- Ensure information is easily searchable and securely shareable
- Collaborate in real time, and remotely, in a digital environment
- Effectively manage asynchronous communication
- Socialize with other staff in a virtual environment using modern platforms
- Support communication and information access on the go securely (e.g., on mobile devices)
- Provide department ownership and control over their content
- Provide user process centric training to ensure effective adoption across staff with varied learning methods and demographics
- Ensure document libraries and migration of documents are aligned with the Commission's Electronic Document Retention and Management (EDRM) plan and recommendations
- Ensure a smooth process for complying with records management policies (e.g., applying document tags and retention policies)
- Apply governance structures that provide effective oversight to ensure a sustainable workplace implementation
- Supply a sustainable and scalable digital workplace architecture and processes to ensure effective ongoing operations
- Guarantee all services comply with the Freedom of Information and Protection of Privacy Act (FOIPPA), IT Infrastructure best practices, Commission's cybersecurity, and record management policies

4. Requirements

4.1 Scope of Services

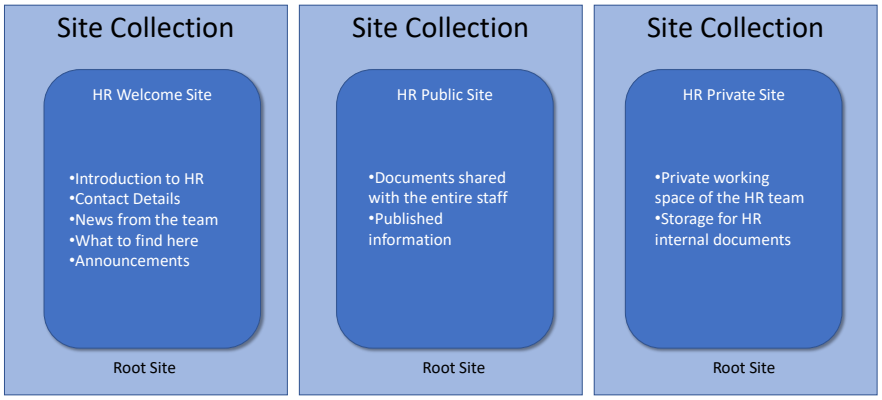
4.1.1 Product Scope

The integration of these M365 services might be visioned as follows:

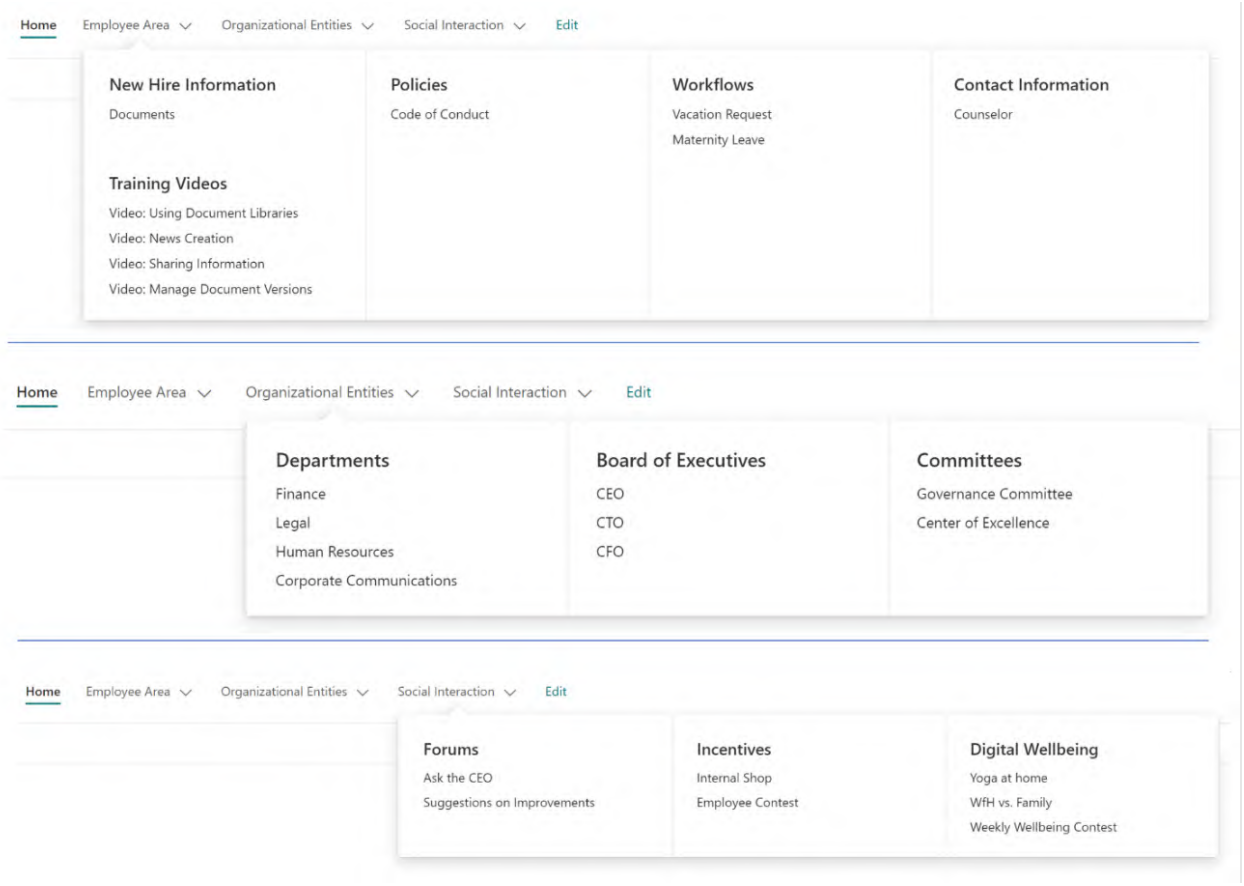


The Commission expects the following to be part of the implementation:

- Technical and Logical SharePoint structure
  - The Commission is leaning towards a flat technical structure (i.e. not using subsites) to ensure ongoing flexibility
  - Sites can include employee facing sites (i.e. corporate), department sites (focused on individual departments), and project sites (focused on cross department teams)
  - An example of a department site using a flat structure might look like the image below:



  - The logical structure (navigation, hierarchy, etc.) will be developed in parallel using the Navigation Mega Menu. An example is shown below:



- Site Templates
  - Develop corporate branding across all pages
    - Common navigation
    - Common theme / colours
    - Unified search
    - Roll-up of News and Events
  - Develop standardized templates for (but not limited to)
    - Landing pages (department welcome pages, employee areas, etc.)
    - Logical subsites (e.g., department public and private pages, project pages)
    - Newsletters
    - News articles
- Multimedia management
  - Implement any multimedia file management tools (such as Streams) to enable easy and secure sharing of multimedia files, such as videos, images
- Document management and migration
  - Assist in migrating documents from shared drives and web servers to OneDrive or SharePoint
  - Assist in converting documents to site pages, where appropriate
  - Ensure records management policies are applied during migration
- Sustainable metadata usage
  - Work with the governance team to set up content within the term store
  - Ensure services implemented (e.g., document libraries) utilize meta data from the term store
  - Help develop policies for meta data usage and incorporate them into the centre of excellence
- Implement search refiners to ensure efficient and relevant content searching
- Collaboration
  - Review and refine the current Teams implementation to ensure effective use of Teams for collaboration and integration into other M365 services
- Socialization Platform
  - Implement a social media platform, such as Yammer, to enable non-business-related conversations
  - Assist in developing governance policies to ensure the platform follows Commission guidelines

- Sharing Corporate Information such as
    - News and Exec Updates
    - Internal staff updates (corporate and department level)
    - Newsletters (corporate and department level)
    - Appropriate combination of tools to publish and share content
- Adoption
    - User/Process centric training materials and adoption plan
    - Identify and develop training materials (including but not limited to recorded training sessions, manuals, short videos, new staff handbook, etc.)
    - Provide training to staff and other Commission trainers
    - Create a detailed plan and execute on change management activities
- Governance and Centre of Excellence
    - Help establish a sustainable centre of excellence and governance structure
    - Help establish a documentation hub for centre of excellence
    - Develop guidelines and best practices to sustainably maintain the centre of excellence
- Security
    - Defined security roles from M365 Global Administrators to End Users
    - A simple three-group security model for sites
        - Site Owners – Full Control
        - Site Members – Edit
        - Site Visitors – Read
    - Company-wide security groups
    - No external sharing of Commission information or data with the possible exception of project sites

The successful proponent is not expected to implement or re-implement:

- Any M365 services the Commission has already implemented, such as Teams
- Any setup of specific records management labels, classification, or policies

4.1.2 Project Scope

The Commission expects this to be a multi-year initiative that is delivered iteratively to realize value early, frequently, and continuously, focusing initially on the implementation of a central corporate portal. In future phases department hub sites and other sites will be introduced. Change management and adoption is expected to be a continuous and ongoing process.

The successful Proponent who enters into a written contract with the Commission is expected to provide the following:

- Project management services using industry best practices for iterative delivery
- Implementation of necessary M365 (and other integrated) services to deliver the scope, including
    - Technical analysis
    - UX and Design proposal
    - Development and implementation of sites and integrations
    - Testing and training technical staff
    - Migration to production
    - Ongoing go-live support
- Expert resources capable of ensuring the project meets objectives through effective and sustainable adoption of new tools
    - Stakeholder engagement and analysis
    - User experience considerations when designing services
    - Provide user training
    - Change management services to help effective adoption
    - Collaboration with Commission staff to transition to operations
    - Set up governance and document best practices
    - Security and privacy consultation when developing components of the digital workplace

The Commission will provide the following

- Collaboration to ensure the project is aligned with intended objectives
- Business and technical product owners of various components of the digital workplace
- Access to business and technical SMEs, stakeholders, and sponsor
- Licensing and necessary access to Commission's M365 tenant
- Project champions to help mediate issues and resolve blockers

4.1.3 Proponent Considerations

The Commission expects all current public health orders, including those issued by the Public Health Officer surrounding the COVID-19 pandemic, are followed. For further details, please see the Commission's website. The proponent must also be able to show proof of COVID vaccination for any on-site meetings.

The Proponent must be able to comply with the following cybersecurity measures. This list is not exhaustive and other measures may be requested during contract signing.

- Contracted project resources must be able to complete work remotely and securely.
- Proponents must be able to supply their team with the tools necessary to access Commission resources, complete project work and interact with Commission staff.
- Proponents may be required to use multi-factor authentication (Microsoft Authenticator or similar) to access Commission resources.

4.2 Content Requirements

To respond to this Request for Proposals, Proponents are required to submit the following information:

- **Qualifications, relevant experience, and proposed team:** Brief relevant experience in delivering M365 services that meets organizational objectives and delivers expected benefits.

- **Proposed Implementation Approach:** Please describe the methodology to be used to deliver scope of services and manage issues. Preference will be given to phased approaches, with timelines and pricing set at a phase level. Include project management approach proposed to manage the implementation approach

- **Adoption Approach:** Describe what methods would be used to ensure the desired project objectives are realized

- **Timelines:** An overall engagement timeline and schedule, including a kick-off date suitable to the Proponent, which is within six weeks after the Closing Date for this RFP allowing time for proposal evaluation.

- **Hourly Rates:** Provide an overall budget for this proposal and clearly state if this is a fixed price or estimated budget. This includes professional fees for each member of the team based on estimated number of hours, including hourly rate. Indicate if there are any travel expenses included in the estimate.

4.3 Format Requirements

The following format, sequence, and instructions should be followed in order to provide consistency in Proponent response and ensure each proposal receives full consideration. With all pages consecutively numbered, the proposals should contain the following parts:

a) Table of contents with page numbers.

b) One-page executive summary.

c) The body of the proposal in accordance with the above content requirements. This part is not to exceed 15 pages of combined text, tables, graphics and other written presentation in support of the content requirements.

5. Evaluation

The evaluation of responses will be conducted by a team consisting of employees and/or contractors of the Commission. All members of the team will be bound by the same standards of confidentiality.

This section details all the mandatory and desirable criteria against which proposals will be evaluated. Proponents should ensure they fully respond to all criteria in order to receive full consideration during the evaluation.

The lowest price or any Proposal will not necessarily be accepted. The Commission reserves the right to refuse any proposal based on quality, service, price, reputation, experience and other criteria.

The Preferred Proponent will be the Proponent scoring the most points after evaluation. The evaluation process will consist of the following stages:

- Stage One – Mandatory Criteria
- Stage Two – Desirable Criteria
- Stage Three – Interviews (optional)
- Stage Four – Reference Checks

5.1 Mandatory Criteria

Proposals not clearly demonstrating they meet the following mandatory criteria will be excluded from further consideration during the evaluation process:

- **The Proposal must be sent and received before the designated closing date and time.**
- **The Proponent must confirm any personal information received, collected or held over the course of the review will be stored and used only in Canada.**
- **The Proposal must contain an independence and objectivity statement by the Proponent.**
- **The Proposal provides a high-level budget and approximate schedule.**
- **The Proposal must include acknowledgement of the following:**
    - Proponents must be able to complete all work remotely and must be able to supply their team with the tools necessary to access Commission resources, complete project work and interact with Commission staff
    - Proponents may be required to use multi-factor authentication (Microsoft Authenticator or similar) to access Commission resources
    - Proponents must be able to show proof of COVID vaccination for any on-site meetings

Failure to meet all mandatory criteria above will disqualify the Proponent's Proposal from further review.

5.2 Desirable Criteria

The Commission seeks to enter into an agreement with the Proponent who, in the opinion of the Commission, has the resources, knowledge and competence to provide the greatest value. Proposals meeting all of the mandatory criteria will be further assessed against desirable criteria.

Desirable Criteria	Weight
Qualifications, relevant experience, and proposed team	20 %
Proposed Implementation Approach	20 %
Proposed Adoption Approach	30 %
Implementation Timeline	10 %
Pricing (Hourly, blended rate – and estimated cost for each implementation phase) e.g. foundations phase, central corporate phase, each department hub/subject area	20 %

5.3 Interviews

The top ranking (to a maximum of three) Proponents may be asked to attend an interview with the evaluation team at a Commission location nearest to the Proponent. The Proponent's team leader is to attend in person. During the interview, the evaluation committee may clarify and/or verify statements made in the written Response.

Interview Criteria	Weight
Understanding of the requirements and implementation plan	30 %
Suitability of resources, their experience, and ability to deliver on the proposed plan to meet project outcomes	30 %
Suitability of change management and adoption approach	40 %

The highest scoring Proponent (Preferred Proponent) will be selected by adding the scores from the desirable criteria and the interview.

The requirement for interviews is optional. The Commission reserves the right to complete the evaluation process without Proponent interviews.

5.4 Reference Checks

The references of the Preferred Proponent may be contacted to validate any part of their responses. The Commission reserves the right to conduct such independent reference checks or verifications as it deems necessary to clarify, test, or verify the information contained in the responses and confirm the suitability of the Proponent. The Commission will not enter into a contract with any Proponent whose references are found to be unsatisfactory.

BC Oil & Gas COMMISSION

Request for Proposals

All enquiries related to this Request for Proposals, including any requests for information and clarification, are to be submitted by **March 18, 2022** and directed, in writing, to **procurement@bcogc.ca,** who will respond if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Commission's option.

RFP #25123001

Electronic File Structures (ARCS/ORCS) for Shared Network Folders

Closing Time: Proposal must be received electronically **before 2:00 PM** Pacific Time on: March 24, 2022

Delivery of Proposals

Proposals must be submitted electronically.

To: https://procurement.bcogc.ca/

Proponent's Meeting

A Proponent's meeting will not be held.

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for overseeing oil and gas operations in British Columbia. Regulatory responsibility is delegated to the Commission through the *Oil and Gas* Activities *Act* and includes specified enactments under the *Forest Act, Heritage Conservation Act, Land Act, Environmental Management Act*, and *Water Act*. The operating costs of the Commission are funded through industry fees and levies on a cost recovery basis.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected by ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

The regulatory responsibility of the Commission extends from the exploration and development phases of oil and gas activities through to facilities operation, and ultimately decommissioning of industry projects. It is charged with balancing a broad range of environmental, economic and social considerations.

A. DEFINITIONS AND ADMINISTRATIVE REQUIREMENTS 4

B. REQUIREMENTS AND RESPONSES 6

1. SUMMARY OF THE REQUIREMENT 6

2. COMMISSION SITUATION/OVERVIEW 6

3. REQUIREMENTS 7

4. EVALUATION 9

5. PROPOSAL FORMAT 9

6. PROPONENT RESPONSE ..... ERROR! BOOKMARK NOT DEFINED.

A. Definitions and Administrative Requirements

1. Definitions

Throughout this Request for Proposals, the following definitions apply:

a) "Contract" means the written agreement resulting from this Request for Proposals executed by the Commission and the Contractor;
b) "Contractor" means the successful Proponent to this Request for Proposals who enters into a written Contract with the Commission;
c) "Must", or "mandatory" means a requirement that must be met in order for a proposal to receive consideration;
d) "Proponent" means an individual or a company that submits, or intends to submit, a proposal in response to this Request for Proposals;
e) "Commission" means the Oil and Gas Commission;
f) "Request for Proposals" means the process described in this document; and
g) "Should" or "desirable" means a requirement having a significant degree of importance to the objectives of the Request for Proposals.

2. Terms and Conditions

Submitting a proposal indicates acceptance of all the terms and conditions set out in the RFP, including those that follow and that are included in all appendices and any Addenda.

A proposal must be signed by a person authorized to sign on behalf of the Proponent with the intent to bind the Proponent to the RFP and to the statements and representations in the Proponent's proposal. A scanned copy of the signed cover page of this RFP is acceptable as is a cover letter identifying the Proponent, identifying the RFP and including a signature of an authorized representative of the Proponent that confirms the Proponent's intent to be bound. For proposals submitted to an electronic proposal constitutes the signature of an authorized representative of the Proponent and is acceptable without additional signature.

3. **Electronic Submissions**

For electronic submissions the following applies:

a) The Proponent is solely responsible for ensuring that the complete electronic Proposal, is received before Closing Time;
b) The maximum size of each attachment must be 500 MB or less and uploaded in a single attachment;
c) Proponents should submit proposal submissions in a single upload and avoid sending multiple submissions for the same opportunity;
d) Attachments must not be compressed, must not contain a virus or malware, must not be corrupted and must be able to be opened. Proponents submitting by electronic submission are solely responsible for ensuring that any emails or attachments are not corrupted. The Commission may reject proposals that are compressed, cannot be opened or that contain viruses or malware or corrupted attachments.

4. Additional Information Regarding the Request for Proposals

All subsequent information regarding this Request for Proposals, including changes made to this document will be posted on the BC Bid website at www.bcbid.ca. It is the sole responsibility of the Proponent to check for amendments on the BC Bid website.

5. Late Proposals

Proposals will be marked with their receipt time once submitted. Only complete proposals received and marked before closing time will be considered to have been received on time. Proposals that are received late will be marked late and will not be considered or evaluated. In the event of a dispute, the proposal receipt time as recorded by the electronic date stamp shall prevail whether accurate or not.

6. **Eligibility**

a) Proposals will not be evaluated if the Proponent's current or past corporate or other interests may, in the Commission's opinion, give rise to a conflict of interest in connection with the project described in this Request for Proposals. This includes, but is not limited to, involvement by a Proponent in the preparation of this Request for Proposals. If a Proponent is in doubt as to whether there might be a conflict of interest, the Proponent should consult with the Commission Contract Management Analyst prior to submitting a proposal.
b) Proposals from not-for-profit agencies will be evaluated against the same criteria as those received from any other Proponents.

7. Evaluation

Evaluation of proposals will be by a committee formed by the Commission and may include employees and contractors of the Commission. All personnel will be bound by the same standards of confidentiality. The Commission's intent is to enter into a Contract with the Proponent who has the highest overall ranking.

8. Negotiation Delay

If a written Contract cannot be negotiated within thirty days of notification of the successful Proponent, the Commission may, at its sole discretion at any time thereafter, terminate negotiations with that Proponent and either negotiate a Contract with the next qualified Proponent or choose to terminate the Request for Proposals process and not enter into a Contract with any of the Proponents.

9. Debriefing

At the conclusion of the Request for Proposals process, all Proponents will be notified of the award by BCBid. Unsuccessful Proponents may request a debriefing meeting with the Commission.

10. Alternative Solutions

If alternative solutions are offered, please submit the information in the same format, as a separate proposal.

11. Changes to Proposals

By submission of a clear and detailed written notification, the Proponent may amend or withdraw its proposal prior to the closing date and time. Upon closing time, all proposals become irrevocable. The Proponent will not change the wording of its proposal after closing and no words or comments will be added to the proposal unless requested by the Commission for purposes of clarification.

12. Proponents' Expenses

Proponents are solely responsible for their own expenses in preparing a proposal and for subsequent negotiations with the Commission, if any. If the Commission elects to reject all proposals, the Commission will not be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the proposal, loss of anticipated profit in connection with any final Contract, or any other matter whatsoever.

13. Limitation of Damages

Further to the preceding paragraph, the Proponent, by submitting a proposal, agrees that it will not claim damages, for whatever reason, relating to the Contract or in respect of the competitive process, in excess of an amount equivalent to the reasonable costs incurred by the Proponent in preparing its proposal and the Proponent, by submitting a proposal, waives any claim for loss of profits if no Contract is made with the Proponent.

14. Proposal Validity

Proposals will be open for acceptance for at least 90 days after the closing date.

15. Firm Pricing

Prices will be firm for the entire Contract period unless this Request for Proposals specifically states otherwise.

16. Currency and Taxes

Prices quoted are to be:

a) In Canadian dollars;
b) Inclusive of duty, where applicable; FOB destination, delivery charges included where applicable; and
c) Exclusive of taxes

17. Completeness of Proposal

By submission of a proposal the Proponent warrants that, if this Request for Proposals is to design, create or provide a system or manage a program, all components required to operate the system or manage the program have been identified in the proposal or will be provided by the Contractor at no charge.

18. Subcontracting

a) Using a subcontractor (who should be clearly identified in the proposal) is acceptable. This includes a joint submission by two Proponents having no formal corporate links. However, in this case, one of these Proponents must be prepared to take overall responsibility for successful performance of the Contract and this should be clearly defined in the proposal.
b) Subcontracting to any firm or individual whose current or past corporate or other interests may, in the Commission's judgment, give rise to a conflict of interest in connection with the project or program described in this Request for Proposals will not be tolerated. This includes, but is not limited to, any firm or individual involved in the formulation of this Request for Proposals. If a Proponent is in doubt as to whether a proposed subcontractor gives rise to a conflict of interest, the Proponent should consult with the Commission Contact Person listed on page 1 prior to submitting a proposal.
c) Where applicable, the names of approved sub-contractors listed in the proposal will be included in the Contract. No additional subcontractors will be added, nor other changes made, to this list in the Contract without the written consent of the Commission.

19. Acceptance of Proposals

a) This Request for Proposals should not be construed as an agreement to purchase goods or services. The Commission is not bound to enter into a Contract with the Proponent who submits the lowest priced proposal or with any Proponent. Proposals will be assessed in light of the evaluation criteria. The Commission will be under no obligation to receive further information, whether written or oral, from any Proponent.
b) Neither acceptance of a proposal nor execution of a Contract will constitute approval of any activity or development contemplated in any proposal that requires any approval, permit or license pursuant to any federal, provincial, regional district or municipal statute, regulation or by-law.

20. Definition of Contract

Notice in writing to a Proponent that it has been identified as the successful Proponent and the subsequent full execution of a written Contract will constitute a Contract for the goods or services, and no Proponent will acquire any legal or equitable rights or privileges relative to the goods or services until the occurrence of both such events.

21. Contract

By submission of a proposal, the Proponent agrees that should its proposal be successful, the Proponent will enter into a Contract with the Commission in accordance with the terms of the Commission's General Service Agreement.

22. Liability for Errors

While the Commission has used considerable efforts to ensure the information in this Request for Proposals is accurate, the information contained in this Request for Proposals is supplied solely as a guideline for Proponents. The information is not guaranteed or warranted to be accurate by the Commission, nor is it necessarily comprehensive or exhaustive. Nothing in this Request for Proposals is intended to relieve Proponents from forming their own opinions and conclusions with respect to the matters addressed in this Request for Proposals.

23. Modification of Terms

The Commission reserves the right to modify the terms of this Request for Proposals at any time in its sole discretion. This includes the right to cancel this Request for Proposals at any time prior to entering into a Contract with the successful Proponent.

24. Ownership of Proposals

All proposals submitted to the Commission become the property of the Commission. They will be received and held in confidence by the Commission, subject to the provisions of the *Freedom of Information and Protection of Privacy Act* and this Request for Proposals.

25. Use of Request for Proposals

Any part of this document, or any information provided by the Commission in relation to this Request for Proposals may not be used or disclosed, for any purpose other than for the submission of proposals. Without limiting the generality of the foregoing, by submission of a proposal, the Proponent agrees to hold in confidence all information provided by the Commission in relation to this Request for Proposals.

26. Reciprocity

The Commission may consider and evaluate any proposals from other jurisdictions on the same basis that the Commission purchasing authorities in those jurisdictions would treat a similar proposal from a British Columbia supplier.

27. No Lobbying

Proponents must not attempt to convey directly or indirectly with any employee, contractor or representative of the Commission, including the evaluation committee and any elected officials of the Commission, or with members of the public or the media, about the project described in this Request for Proposals or otherwise in respect of the Request for Proposals, other than as expressly directed or permitted by the Commission.

B. Requirements and Responses

1. Summary of the Requirement

The BC Oil and Gas Commission (Commission) requires a Records & Information Management (RIM) expert to organize a high volume of electronic records on a shared network drive. This organization is to be completed by developing new folder structures that conform to the requirements of the *Information Management Act* (IMA) through the implementation of the BC government's Administrative Records Classification Schedule (ARCS) framework and Commission's Operational Records Classification System (ORCS). The objective is to attain a state of Electronic Document & Records Management System (EDRMS) readiness, where the Commission's electronic records are appropriately classified in accordance with ARCS/ORCS and identified by standardized naming conventions at the folder level in preparation for future migration. The work is to be performed across the Commission on a branch by branch (business unit) basis, although simultaneous management of two or more projects may be required to maximize time and productivity. Oversight and direction will be provided by the Commission's internal Records & Information Services Branch, including the order and prioritization of projects for completion.

2. Anticipated Schedule

The following table outlines the anticipated schedule for this RFP. All times identified in the table are in Pacific Time.

Event	Anticipated Date
Enquiries deadline	March 18, 2022
Request closing time	March 24, 2022 2:00 PM PT
Reference checks, as required	March 28-April 1, 2022
Preferred Proponent selected by	April 4, 2022
Commencement of work	April, 2022

3. Commission Situation/Overview

The Commission is the provincial regulatory agency for permitting and overseeing oil and gas activities, from exploration and development through to operations and ultimately decommissioning of oil and gas industry projects under British Columbia jurisdiction. The Commission's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2021/22 – 2023/24 Service Plan available on the Commission's website at www.bcogc.ca.

3.1 Commission Responsibility

The purposes of the Commission, outlined in Section 4 of the Oil and Gas Activities Act, are briefly summarized as follows:

(a) to regulate oil and gas activities in British Columbia in a manner that
  (i) provides for the sound development of the oil and gas sector, by fostering a healthy environment, a sound economy and social well-being,
  (ii) conserves petroleum and natural gas resources,
  (iii) ensures safe and efficient practices, and
  (iv) assists owners of petroleum and natural gas resources to participate equitably in the production of shared pools of petroleum and natural gas;

(b) to provide for effective and efficient processes for the review of applications for permits and to ensure that applications that are approved are in the public interest having regard to environmental, economic and social effects;

(c) to encourage the participation of First Nations and aboriginal peoples in processes affecting them;

(d) to participate in planning processes;

(e) to undertake programs of education and communication in order to advance safe and efficient practices and the other purposes of the commission.

3.2 Background

The Commission has modernized its Operational Records Classification System (ORCS) to reflect its current mandate, lines of business, and the records that support these. The amended records schedule (Schedule 163507, Amendment 144019) received approval by the provincial Chief Records Officer in March 2019.

Implementation of ARCS and ORCS within the Commission's unstructured electronic records environment has been identified as a critical initiative to support the organization's ongoing transition to Microsoft Office 365 (M365) and future planned migration of records from the shared drive to the new platform. The ARCS and ORCS implementation work has been initiated and completed in some branches, however, a significant number of business units have yet to be supported.

The Commission's goal is to complete implementation of ARCS and ORCS across all branches of the organization.

4. Requirements

4.1 Scope of Services

The services outlined in this Request for Proposals (RFP) are anticipated to commence April 2022 and complete on March 31, 2023 within a maximum contract amount of $75,000.00. The Commission has discretion to offer the proponent a one-year renewal of services in fiscal 2022/23.

The successful Proponent will be expected to use Microsoft Teams to support regular engagement with the Commission's Records Management team and branch staff in the various Commission offices (Victoria, Fort St. John, Kelowna, Prince George, Dawson Creek, and Terrace). Travel will not be required. All meetings with staff will be conducted remotely and project work will be completed offsite using a Commission issued user ID and laptop. An exception to the offsite arrangement might apply if the successful Proponent is located in Victoria, BC and ad hoc in-person meetings are mutually agreed upon by all parties.

The successful Proponent will be expected to comply with the Commission's COVID-19 Vaccination Policy for External Visitors/Contractors as a condition of the contract. Information on the Commission's vaccination requirements is available here.

The successful Proponent who enters into a written contract with the Commission will be responsible for the following services:

Establishment of folder structures and folder naming conventions:

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions
- Moving folders and associated records to the new folder structure (with user acceptance/permission)
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary using Commission approved software (Tree Size)
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

User support, training and change management:

- Effectively initiating each electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training (formal or desk-side) to staff on the use and maintenance of the new shared drive folder structure

Project reporting and monitoring:

- Providing briefings and status updates as and when requested
- Maintaining project progress and completion metrics to support statistical reporting and final results
- Maintaining a current work plan and project schedule

4.2 Content Requirements

To respond to this Request for Proposals, Proponents are required to submit the following information:

A. Proposed Approach

1) Provide a description of the methodology (approach) that will be followed to successfully develop electronic filing structures for Commission clients based on ARCS/ORCS
2) Describe how clients will be supported through the project as they transition from their old filing structure to the new structure
3) Describe how clients will be trained on using and maintaining the new filing structure once implemented (e.g. describe and/or include samples of any guidelines, training tools, aids, etc.)
4) Describe how project progress will be tracked and measured to ensure timeliness and quality of deliverables

B. Proposed Proponent, Qualifications and Hourly Rate

1) Provide the name of proposed individual to complete work (1 individual only)
2) Provide a brief description of your (or named individual) qualifications and abilities relevant to the services outlined
3) Provide hourly rate for services
4) Provide two satisfied client references, including name, title, organization, phone number, email address and date that you (or named individual) worked for these clients

C. Relevant Experience

Please provide answers to the following:

1) What work experience do you (or named individual) have with respect to implementing ARCS and/or ORCS schedules in a BC government setting? Include a brief description of the government organization(s), nature of work performed, when the work was completed, and in what capacity.
2) What experience do you (or named individual) have delivering electronic file structure projects? Include a brief description of a project(s) that included organizing electronic folders and/or documents on a shared drive and applying record schedules.
3) Was your (or named individual) project(s) specific to preparing electronic records for future migration to an Electronic Document & Records Management System (EDRMS) or Microsoft Office 365? Was your (or named individual) project(s) successfully completed? Include a brief description of how success was determined or measured.

4.3 Format Requirements

The following format, sequence, and instructions should be followed in order to provide consistency in Proponent response and ensure each proposal receives full consideration. With all pages consecutively numbered, the proposals should contain the following parts:

a) Table of contents with page numbers.

b) One-page executive summary.

c) The body of the proposal in accordance with the above content requirements. This part is not to exceed 10 pages of combined text, tables, graphics and other written presentation in support of the content requirements.

5. Evaluation

The evaluation of responses will be conducted by a team consisting of employees and/or contractors of the Commission. All members of the team will be bound by the same standards of confidentiality.

This section details all of the mandatory and desirable criteria against which proposals will be evaluated. Proponents should ensure that they fully respond to all criteria in order to receive full consideration during the evaluation.

The lowest price or any Proposal will not necessarily be accepted. The Commission reserves the right to refuse any proposed based on quality, service, price, reputation, experience and other criteria.

The Preferred Proponent will be the Proponent scoring the most points after evaluation. The evaluation process will consist of the following stages:

- Stage One – Mandatory Criteria
- Stage Two – Desirable Criteria
- Stage Three – Reference Checks (optional)

5.1 Mandatory Criteria

Proposals not clearly demonstrating that they meet the following mandatory criteria will be excluded from further consideration during the evaluation process:

- **The Proposal must be sent and received before the designated closing date and time.**
- **The Proponent must confirm that any personal information received, collected or held over the course of the review will be stored and used only in Canada.**
- **The Proposal must contain an independence and objectivity statement by the Proponent.**
- **The Proposal must confirm compliance with the Commission's vaccination policy.**

Failure to meet all mandatory criteria above will disqualify the Proponent's Proposal from further review.

5.2 Desirable Criteria

The Commission seeks to enter into an agreement with the Proponent who, in the opinion of the Commission, has the resources, knowledge and competence to provide the greatest value. Proposals meeting all of the mandatory criteria will be further assessed against desirable criteria.

Desirable Criteria	Weight
Proponent's Qualifications and Relevant Experience	35%
Suitability of Proposed Approach	35%
Pricing Hourly rate for services	30%

5.3 Reference Checks

The references of the Preferred Proponent may be contacted to validate any part of their responses. The Commission reserves the right to conduct such independent reference checks or verifications as they deem necessary to clarify, test, or verify the information contained in the responses and confirm the suitability of the Proponent. The Commission will not enter into a contract with any Proponent whose references are found to be unsatisfactory.

Reference Check Criteria	Weight
Client satisfaction with Proponent services and/or verification of Proposal responses	Pass/Fail

BRITISH COLUMBIA **ENERGY REGULATOR**

Request for Information: RFI# 21524001

The BC Energy Regulator ("BCER") is requesting information from interested parties that can provide Records & Information Management (RIM) consultant services to organize a high volume of electronic records on a shared network drive. This organization is to be completed by developing new folder structures that conform to the requirements of the B.C. *Information Management Act* (IMA) through the implementation of the B.C. government's Administrative Records Classification Schedule (ARCS) framework and BCER's Operational Records Classification System (ORCS). The objective is to ensure electronic records are appropriately classified according to ARCS/ORCS and identified by standardized naming conventions at the folder level.

Project oversight and direction will be provided by the BCER's internal Records & Information Services Branch, including coordination and prioritization of projects for completion.

The process will involve use of the software tool TreeSize Professional or a comparable product to identify and support deletion of duplicate files and address long file paths. User support, training and change management are deemed integral to project success.

The work is to be performed across the organization on a branch by branch (business unit) basis. While the ARCS and ORCS implementation work has been completed in some branches, a significant number have yet to be supported. Use of Microsoft Teams will support regular engagement with the internal Records team and BCER branch staff in the various offices (Victoria, Fort St. John, Kelowna, Prince George, Dawson Creek, and Terrace). Travel would not be required.

Implementation of ARCS/ORCS within the BCER's unstructured electronic records environment has been identified as a critical initiative to support the organization's ongoing transition to Microsoft Office 365 (M365) and migration of records from the shared drive to the new platform, with SharePoint as the current EDRM solution.

Organizational Vision and Mission

The BCER regulates the full life cycle of energy resource activities in B.C., from site planning to restoration. We ensure activities are undertaken in a manner that protects public safety, safeguards the environment, supports meaningful reconciliation, and advances the public interest and contributes to B.C.'s economy. The BCER's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2023/24 - 2025/26 Service Plan available on the BCER's website at www.bc-er.ca.

The BCER mission is as follows:

We regulate the life cycle of energy resource activities in B.C. from site planning to restoration, ensuring activities are undertaken in a manner that:

- Protects public safety and the environment
- Supports reconciliation with Indigenous peoples and the transition to a low-carbon economy
- Fosters a sound economy and social well-being

BRITISH COLUMBIA ENERGY REGULATOR

Request for Information: RFI# 21524001

RFI Objective

This RFI seeks to locate service providers that would have the resources, skills and experience to complete this specialized work at a competitive price.

Interested parties are invited to respond to this RFI by submitting a response to the BCER by **June 30, 2023**.

Respondents are requested to provide a concise and focused response to this RFI. Responses are requested in the following format:

a) brief company/consultant profile including a description of comparable projects and/or relevant qualifications (1 page maximum)
b) name of a key contact person, including telephone number, Email address and physical location
c) identification and discussion of key factors related to the scope of work as outlined
d) high-level cost and/or rate estimates
e) consultant availability
f) other required information specific to the nature of this RFI and deemed important by the respondent

This RFI may be used to pre-qualify or screen service providers for a subsequent competitive bidding process, if any.

If subsequent competitive bidding opportunities are issued, the BCER is under no obligation to advise any service provider responding to this RFI. Service providers are advised to monitor the B.C. Bid website (https://www.new.bcbid.gov.bc.ca) or the BCER's procurement page (https://procurement.bc-er.ca/) for any such opportunities, which will be open to all service providers regardless of whether or not a response to this RFI has been submitted.

All responses to this RFI become the property of the BCER and will be held in confidence, subject to the provisions of the *Freedom of Information and Protection of Privacy Act*. Respondents to this RFI consent to the BCER incorporating any submitted information (e.g., approaches or methodologies) into any planning, procurement, or contractual activities related to any aspect of the project without any obligation, liability, or consideration on the part of the BCER. The BCER will not be responsible for any costs incurred by any service provider in responding to this RFI.

Responses should be delivered to https://procurement.bc-er.ca/ **before 2:00 p.m. Pacific Time on June 30, 2023**, and should reference RFI# 21524001.

All enquiries related to this Request for Information, including any requests for clarification, are to be submitted by **June 26, 2023** and directed, by Email, to procurement@bc-er.ca, who will provide responses on https://procurement.bc-er.ca/ if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all respondents at the BCER's option.

Request for Proposals

All enquiries related to this Request for Proposals, including any requests for information and clarification, are to be submitted by **December 14, 2022** and directed, in writing, to **procurement@bcogc.ca,** who will respond if time permits. Information obtained from any other source is not official and should not be relied upon. Enquiries and any responses will be recorded and may be distributed to all Proponents at the Commission's option.

RFP # 21523001

Document Scanning Services – Well Authorization File Conversion

Closing Time: Proposal must be received electronically **before 2:00 PM** Pacific Time on: **December 29, 2022**

Delivery of Proposals

Proposals must be submitted electronically.

To: https://procurement.bcogc.ca/

Proponent's Meeting

A Proponent's meeting will not be held.

Organization Overview

The BC Oil and Gas Commission (Commission) is the Province of B.C.'s life-cycle energy resources regulator. The Commission is a Crown agency with a mandate to ensure both the environment and public safety are protected, and those with concerns have the opportunity to have their voices heard in the sustainable development of British Columbia's energy resources.

As a cost recoverable, values driven organization, we prioritize safety, stewardship, and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The Commission is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), the Declaration on the Rights of Indigenous Peoples Act, and the Truth and Reconciliation Commission's (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the Commission delivers on Government's priorities.

The Commission has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the Commission is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as the foundation of our respectful culture. Secured access to Commission information and systems is a foundational consideration in the management of the Commission's infrastructure.

A. DEFINITIONS AND ADMINISTRATIVE REQUIREMENTS 4
B. REQUIREMENTS AND RESPONSES 6
1. SUMMARY OF THE REQUIREMENT 6
2. COMMISSION SITUATION/OVERVIEW 6
3. REQUIREMENTS 7
4. EVALUATION 12
5. PROPOSAL FORMAT 13
6. PROPONENT RESPONSE 11

A. Definitions and Administrative Requirements

1. Definitions

Throughout this Request for Proposals, the following definitions apply:
"Contract" means the written agreement resulting from this Request for Proposals executed by the Commission and the Contractor;
"Contractor" means the successful Proponent to this Request for Proposals who enters into a written Contract with the Commission;
"Must", or "mandatory" means a requirement that must be met in order for a proposal to receive consideration;
"Proponent" means an individual or a company that submits, or intends to submit, a proposal in response to this Request for Proposals;
"Commission" means the Oil and Gas Commission;
"Request for Proposals" means the process described in this document; and
"Should" or "desirable" means a requirement having a significant degree of importance to the objectives of the Request for Proposals.

2. Terms and Conditions

Submitting a proposal indicates acceptance of all the terms and conditions set out in the RFP, including those that follow and that are included in all appendices and any Addenda.

A proposal must be signed by a person authorized to sign on behalf of the Proponent with the intent to bind the Proponent to the RFP and to the statements and representations in the Proponent's proposal. A scanned copy of the signed cover page of this RFP is acceptable as is a cover letter identifying the Proponent, identifying the RFP and including a signature of an authorized representative of the Proponent that confirms the Proponent's intent to be bound. For proposals submitted to an electronic proposal constitutes the signature of an authorized representative of the Proponent and is acceptable without additional signature.

3. Electronic Submissions

For electronic submissions, the following applies:
a) The Proponent is solely responsible for ensuring that the complete electronic Proposal, is received before Closing Time;
b) The maximum size of each attachment must be 500 MB or less and uploaded in a single attachment;
c) Proponents should submit proposal submissions in a single upload and avoid sending multiple submissions for the same opportunity;
d) Attachments must not be compressed, must not contain a virus or malware, must not be corrupted and must be able to be opened.

Proponents submitting by electronic submission are solely responsible for ensuring that any emails or attachments are not corrupted. The Commission may reject proposals that are compressed, cannot be opened or that contain viruses or malware or corrupted attachments.

4. Additional Information Regarding the Request for Proposals

All subsequent information regarding this Request for Proposals, including changes made to this document will be posted on the BC Bid website at www.bcbid.ca. It is the sole responsibility of the Proponent to check for amendments on the BC Bid website.

5. Late Proposals

Proposals will be marked with their receipt time once submitted. Only complete proposals received and marked before closing time will be considered to have been received on time. Proposals that are received late will be marked late and will not be considered or evaluated. In the event of a dispute, the proposal receipt time as recorded by the electronic date stamp shall prevail whether accurate or not.

6. Eligibility

a) Proposals will not be evaluated if the Proponent's current or past corporate or other interests may, in the Commission's opinion, give rise to a conflict of interest in connection with the project described in this Request for Proposals. This includes, but is not limited to, involvement by a Proponent in the preparation of this Request for Proposals. If a Proponent is in doubt as to whether there might be a conflict of interest, the Proponent should consult with the Commission Contract Management Analyst prior to submitting a proposal.
b) Proposals from not-for-profit agencies will be evaluated against the same criteria as those received from any other Proponents.

7. Evaluation

Evaluation of proposals will be by a committee formed by the Commission and may include employees and contractors of the Commission. All personnel will be bound by the same standards of confidentiality. The Commission's intent is to enter into a Contract with the Proponent who has the highest overall ranking.

8. Negotiation Delay

If a written Contract cannot be negotiated within thirty days of notification of the successful Proponent, the Commission may, at its sole discretion at any time thereafter, terminate negotiations with that Proponent and either negotiate a Contract with the next qualified Proponent or choose to terminate the Request for Proposals process and not enter into a Contract with any of the Proponents.

9. Debriefing

At the conclusion of the Request for Proposals process, all Proponents will be notified of the award by BCBid. Unsuccessful Proponents may request a debriefing meeting with the Commission.

10. Alternative Solutions

If alternative solutions are offered, please submit the information in the same format, as a separate proposal.

11. Changes to Proposals

By submission of a clear and detailed written notification, the Proponent may amend or withdraw its proposal prior to the closing date and time. Upon closing time, all proposals become irrevocable. The Proponent will not change the wording of its proposal after closing and no words or comments will be added to the proposal unless requested by the Commission for purposes of clarification.

12. Proponents' Expenses

Proponents are solely responsible for their own expenses in preparing a proposal and for subsequent negotiations with the Commission, if any. If the Commission elects to reject all proposals, the Commission will not be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the proposal, loss of anticipated profit in connection with any final Contract, or any other matter whatsoever.

13. Limitation of Damages

Further to the preceding paragraph, the Proponent, by submitting a proposal, agrees that it will not claim damages, for whatever reason, relating to the Contract or in respect of the competitive process, in excess of an amount equivalent to the reasonable costs incurred by the Proponent in preparing its proposal and the Proponent, by submitting a proposal, waives any claim for loss of profits if no Contract is made with the Proponent.

14. Proposal Validity
Proposals will be open for acceptance for at least 90 days after the closing date.

15. Firm Pricing
Prices will be firm for the entire Contract period unless this Request for Proposals specifically states otherwise.

16. Currency and Taxes
Prices quoted are to be:
a) In Canadian dollars;
b) Inclusive of duty, where applicable; FOB destination, delivery charges included where applicable; and
c) Exclusive of taxes

17. Completeness of Proposal
By submission of a proposal the Proponent warrants that, if this Request for Proposals is to design, create or provide a system or manage a program, all components required to operate the system or manage the program have been identified in the proposal or will be provided by the Contractor at no charge.

18. Subcontracting
a) Using a subcontractor (who should be clearly identified in the proposal) is acceptable. This includes a joint submission by two Proponents having no formal corporate links. However, in this case, one of these Proponents must be prepared to take overall responsibility for successful performance of the Contract and this should be clearly defined in the proposal.
b) Subcontracting to any firm or individual whose current or past corporate or other interests may, in the Commission's judgment, give rise to a conflict of interest in connection with the project or program described in this Request for Proposals will not be tolerated. This includes, but is not limited to, any firm or individual involved in the formulation of this Request for Proposals. If a Proponent is in doubt as to whether a proposed subcontractor gives rise to a conflict of interest, the Proponent should consult with the Commission Contact Person listed on page 1 prior to submitting a proposal.
c) Where applicable, the names of approved sub-contractors listed in the proposal will be included in the Contract. No additional subcontractors will be added, nor other changes made, to this list in the Contract without the written consent of the Commission.

19. Acceptance of Proposals
a) This Request for Proposals should not be construed as an agreement to purchase goods or services. The Commission is not bound to enter into a Contract with the Proponent who submits the lowest priced proposal or with any Proponent. Proposals will be assessed in light of the evaluation criteria. The Commission will be under no obligation to receive further information, whether written or oral, from any Proponent.
b) Neither acceptance of a proposal nor execution of a Contract will constitute approval of any activity or development contemplated in any proposal that requires any approval, permit or license pursuant to any federal, provincial, regional district or municipal statute, regulation or by-law.

20. Definition of Contract
Notice in writing to a Proponent that it has been identified as the successful Proponent and the subsequent full execution of a written Contract will constitute a Contract for the goods or services, and no Proponent will acquire any legal or equitable rights or privileges relative to the goods or services until the occurrence of both such events.

21. Contract
By submission of a proposal, the Proponent agrees that should its proposal be successful, the Proponent will enter into a Contract with the Commission in accordance with the terms of the Commission's General Service Agreement.

22. Liability for Errors
While the Commission has used considerable efforts to ensure the information in this Request for Proposals is accurate, the information contained in this Request for Proposals is supplied solely as a guideline for Proponents. The information is not guaranteed or warranted to be accurate by the Commission, nor is it necessarily comprehensive or exhaustive. Nothing in this Request for Proposals is intended to relieve Proponents from forming their own opinions and conclusions with respect to the matters addressed in this Request for Proposals.

23. Modification of Terms
The Commission reserves the right to modify the terms of this Request for Proposals at any time in its sole discretion. This includes the right to cancel this Request for Proposals at any time prior to entering into a Contract with the successful Proponent.

24. Ownership of Proposals
All proposals submitted to the Commission become the property of the Commission. They will be received and held in confidence by the Commission, subject to the provisions of the *Freedom of Information and Protection of Privacy Act* and this Request for Proposals.

25. Use of Request for Proposals
Any part of this document, or any information provided by the Commission in relation to this Request for Proposals may not be used or disclosed, for any purpose other than for the submission of proposals. Without limiting the generality of the foregoing, by submission of a proposal, the Proponent agrees to hold in confidence all information provided by the Commission in relation to this Request for Proposals.

26. Reciprocity
The Commission may consider and evaluate any proposals from other jurisdictions on the same basis that the Commission purchasing authorities in those jurisdictions would treat a similar proposal from a British Columbia supplier.

27. No Lobbying
Proponents must not attempt to convey directly or indirectly with any employee, contractor or representative of the Commission, including the evaluation committee and any elected officials of the Commission, or with members of the public or the media, about the project described in this Request for Proposals or otherwise in respect of the Request for Proposals, other than as expressly directed or permitted by the Commission.

B. Requirements and Responses

1. Summary of the Requirement

The BC Oil and Gas Commission (Commission) is seeking responses from this Request for Proposal (RFP) for document scanning services. A qualified digital imaging (scanning) service provider is required to convert a large collection of Well Authorization files from paper to digital form.

Well Authorization files (well files) include historical geological and technical well information related to provincial oil and gas activities. The files date from the early 1950's to 2014 and comprise the Commission's only record copy. The information contained within the collection is critical for managing the lifecycles of BC wells and supporting future oil and gas exploration.

Physical security, safe handling and preservation of file material during all phases of scanning service delivery is of utmost importance. File integrity must be maintained as all hardcopy records will be returned to the source storage facility and retained indefinitely post-digitization.

The well files hold a range of standard (8½ x 11), legal, large and irregular size document types, each requiring specialized scanning equipment. The successful Proponent will be required to use Commission approved equipment and adhere to established imaging standards for the duration of the project.

Well files for the project are located at government contracted offsite storage facilities in Victoria, British Columbia. The successful Proponent will be located in Victoria or the southern Vancouver Island area, and all scanning services will be completed locally to limit the transport of records. Approximately 4000-4500 boxes of Commission well files require scanning. This contract will be a first step of what is recognized as a longer-term digitization initiative.

Work on this project will be initiated as soon as possible in fiscal 2022/23 and is subject to continuation through 2023/24 upon approved funding. Project oversight and direction will be provided by the Commission's Records & Information Services (RIS) Branch, including the prioritization and ordering of records boxes for scanning.

2. Anticipated Schedule

The following table outlines the anticipated schedule for this RFP. All times identified in the table are in Pacific Time.

Event	Anticipated Date
Project enquiries deadline	December 14, 2022
Site visit request/scheduling deadline	December 12, 2022
One (1) hour site visits for file viewing	December 8,12-13, 2022
Request for Proposal (RFP) closing time	December 29, 2022 2:00 PM PT
Inspection of Proponent facilities	Week of January 2-5, 2023
Reference checks (as required)	Week of January 2-5, 2023
Preferred Proponent selected by	January 5, 2023
Contract finalization / anticipated project start	Week of January 9-13, 2023

3. Commission Situation/Overview

The Commission is the provincial regulatory agency for permitting and overseeing oil and gas activities, from exploration and development through to operations and ultimately decommissioning of oil and gas industry projects under British Columbia jurisdiction. The Commission's current legislated mandate, regulatory framework, core activities and organizational structure are described in the 2021/22 – 2023/24 Service Plan available on the Commission's website at www.bcogc.ca.

3.1 Commission Responsibility

The Commission mission is as follows:

We regulate the life cycle of energy resource activities in B.C. from site planning to restoration, ensuring activities are undertaken in a manner that:

- Protects public safety
- Safeguards the environment
- Supports meaningful reconciliation
- Advances the public interest and contributes to B.C's economy

3.2 Background

The Commission's Well Authorization files (well files) directly support the Commission's mandate to regulate and monitor the exploration and development of oil and gas activities in British Columbia (B.C.), including the management, long term protection and conservation, control and treatment of wells.

Well file records are retained for an indefinite period as well integrity issues can arise long after a well is considered remediated or "closed". In these situations, immediate access to the file is necessary to manage safety and environmental issues. Data connected with or derived from drilling, production or other work performed on a well is maintained within these files.

Within B.C., the legislative landscape for managing information assets has evolved to support the shift from paper records to those in digital format. The *Information Management Act* (IMA) provides the mandate for improved information management practices and modernization across the provincial government. The IMA requires the digitization of non-digital records (subject to specific exemptions) to make government public bodies more efficient and support digital end-to-end services that meet public needs.

Conversion of the well files from paper to digital format is a corporate priority as the Commission transitions to a digital organization. The majority of scanning work is managed by a dedicated full-time equivalent (FTE) employee within the RIS Branch (Well File Technician). Files are routinely retrieved from one of two government contracted storage facilities in Victoria (Cube Global Storage and Access Records Storage) and scanned using specialized equipment in the Commission's Victoria office location.

Through this project, valuable historical well data will become more readily accessible to our industry stakeholders and the public.

4. Requirements

4.1 Scope of Services

Eligibility:

To be eligible to respond to this RFP, the proposing service provider shall: (a) reside in Victoria, BC or one of the surrounding municipalities of Southern Vancouver Island; (b) have a minimum of 5 years experience in the conversion of hardcopy documents to digital images for computer processing.

The Commission reserves the right to request live demonstrations of the proposed services to be performed and inspect the service provider's facility in making a determination of their ability and capacity to perform the requirements of the RFP.

Contract Term:

The initial contract term is anticipated to commence in January 2023 and complete on March 31, 2023. The Commission reserves the right to continue services and extend the contract for up to an additional one (1) year term pending a budget review in April 2023 and providing all terms, conditions and specifications remain the same and both parties agree to the extension.

In the event services are scheduled to end because of the expiration of this contract, the successful Proponent shall continue the service upon written request by the Director, Records & Information Services. The extension period shall not continue for more than ninety (90) days beyond the expiration date of the existing contract. The successful proponent will be compensated for the service at the rate in effect if this extension clause is invoked by the Commission.

Budget:

The Commission has funding available for scanning services completed in fiscal 2022/23. The objective is to digitize as many boxes of well files as possible by March 31, 2023. A subsequent budget review will be conducted in April 2023 to support a continuation of services for fiscal 2023/24.

Service Test Period:

The Commission reserves the right to require a test period (paid) to determine if the successful Proponent can perform in accordance with the requirements of the contract and to the Commission's satisfaction. Such a test period can be from thirty (30) to sixty (60) days, and will be conducted under all specifications, terms and conditions contained in the contract.

A performance evaluation will be conducted prior to the end of the test period and that evaluation will be the basis for the Commission's decision to continue with the successful Proponent or to terminate the contract and select another service provider.

Site Visits for File Viewing – COVID-19 Policy:

Proponents may request an onsite visit to preview a sampling of the Well Authorization files and documents covered in this RFP.

Visits may be scheduled on **December 8, 12 or 13** and are not to exceed one (1) hour in duration. The location for site visits is 2950 Jutland Rd., Victoria, BC. The contact for scheduling a site visit is Kathryn Smerechinskiy, Director, Records and Information Management: Kathryn.Smerechinskiy@bcogc.ca. All requests for site visits should be received by the Commission by **December 12**.

All visitors to the Victoria office will be expected to comply with the Commission's COVID-19 Vaccination Policy for External Visitors/Contractors (Policy) as a condition of the visit. Information on the Commission's vaccination and verification requirements is available here. Masks are optional. Failure to comply with any condition of the Policy will result in cancellation of the scheduled visit.

Service Requirements:

The successful Proponent who enters into a written contract with the Commission will be responsible for the following as part of contracted services:

1. Storage facility liaison
    - The Proponent will liaise with the Commission's RIS Branch contact to coordinate the retrieval and return of file boxes to/from a storage facility.
    - Facility processes and requirements for retrieving, receiving and returning boxes should be respected and adhered to.
    - All file box retrievals and returns must be done in a secure manner where Commission records are not left unattended.
    - All facility staff and associated drivers should be treated respectfully and provided clear direction related to the delivery and retrieval of boxes.
    - Box transfer/shipping documentation must be signed and retained by the Proponent as evidence of each box's physical whereabouts and current custodianship.
    - Any issue or incident related to box retrievals or returns involving a storage facility (staff or driver) should be immediately reported to the Commission for action (RIS Branch Director).

2. Onsite box management
   - Received file boxes must be maintained in a secure locked and dry environment that is free from any potential risk of damage while in the Proponent's custody.
   - Proponent location/facility must have adequate fire alarm systems, fire protected areas, and response measures in place.
   - Only authorized staff are to have access to Commission files.
   - Careful handling of file boxes, files and documents is expected in recognition of the collection's value and age, and awareness that these comprise the Commission's only record copies.

3. Rush/priority requests for files
   - Upon request, Proponent will be expected to expeditiously locate and coordinate the physical transfer of requested file(s) in their custody or prioritize data digitization for electronic transfer to the Commission.

4. Document preparation – Pre-scanning
   - Preparation of files for scanning includes:
     a. removing all staples, clips and other fasteners from single and multi-page documents (through use of appropriate tools to prevent tearing or otherwise damaging the documents)
     b. checking the numerical sequence and order of pages in multi-page documents
     c. verifying that all pages/documents are facing the same direction and are right side up
     d. re-stapling/re-clipping documents in the same original order after completion of scanning
     e. removing any report binding (unbinding) and file backing sheets
     f. moving post-it notes as necessary to ensure document content isn't obscured
     g. carefully unfolding large and irregular size documents to prevent tearing
     h. photocopying torn, brittle, faint, or thin documents (when feasible based on document size) or enclosing fragile originals in protective plastic sleeves
     i. repairing any torn documents with tape

5. Document/file restoration – Post-scanning
   - Post-scanning standards for returning files to offsite storage are:
     a. documents are returned to the correct file folder in the correct order
     b. file folders are returned to the correct file box
     c. files within each box are arranged in numerical order by the Well Authorization number (e.g. WA12345)

6. Data capture/images
   - Each document type within a file will be scanned separately in the format required (e.g. PDF, Tiff).
   - Scanning will cover single-sided and double-sided documents, as required.
   - Where a document type consists of multiple pages, all pages will be scanned.
   - Document pages will be rotated as needed to ensure proper orientation and maximum readability.

7. Quality control/image quality assurance (QA)
   - Scanned documents will be checked for quality and conformity prior to their submittal to the Commission, for example:
     a. any pages found not oriented properly will be appropriately rotated
     b. Any distorted images will be re-digitized
     c. Any blank pages will be deleted
     d. Colour accurately compares with the original document
   - Text and/or graphic images that can be read on an original document must be as readable on the scanned image.

     In the event that a source document is not clear and legible, or a clear and legible reproduction cannot be produced, the successful Proponent is required to inform the Commission Records branch contact and provide an overview of the document in question.

8. Data transfer
   - File data will be submitted to the Commission through secure file transfer protocol (FTP) as directed.
   - Uploaded data to the FTP will be organized as follows:
     a. one folder created per Well Authorization file
     b. each folder will be named according to the unique Well Authorization number (e.g. WA 12345)
     c. all documentation will be saved to the appropriate well file folder (folder must include all documents related to the well, including those spanning multiple volumes)

9. Status reporting and box/file tracking:
   - Providing briefings and status updates as requested.
   - Maintaining a current work plan, schedule, and tracking tool that supports the accurate location and retrieval of a box/file at any stage of the process.
   - Maintaining project progress and completion metrics.
   - Consulting with the Commission's RIS Branch staff as necessary to support contract deliverables.

10. Project meetings:
    - Any meetings with Commission staff will be conducted remotely using Microsoft Teams (e.g. start up, regular engagement or status updates). An exception to the offsite arrangement may apply if an ad hoc in-person meeting is mutually agreed upon by all parties.

Scanning Equipment Requirements:

The successful Proponent who enters into a written contract with the Commission is expected to use scanning equipment comparable in quality and performance to **a**. and **b.** below, and is required to use equipment listed in **c.** below as a condition of the contract for services:

a. Fujitsu Image Desktop scanner (Model: fi-7800)
b. Contex SD One MF 44" wide format colour scanner
c. **NeuraScanner** (See Well Log Scanner | Log Scanners | Large Portable Scanners (neuralog.com) and neuralog-products-solutions.pdf for details)

The Commission requires the successful Proponent to use Neuralog's **NeuraScanner** for digitizing well and formation evaluation logs. Costs incurred through the procurement (or lease, if available) of a NeuraScanner are to be solely borne by the Proponent. Contact www.neuralog.com for information:

Headquarters North America - US & Canada

4800 Sugar Grove Blvd., Suite 200

Houston, TX USA
sales@neuralog.com
1-281-240-2525 Office
1-800-364-8728 Toll Free (US and Canada)

Well File Overview:

There are approximately 5,000 boxes of well files located in offsite storage. Of these, some 4000-4,500 boxes require digitization.

Well file boxes consist of standard size banker boxes (12"x10"x15"). Each box of files varies in the type and volume of documents. The number of individual well files in a box also varies significantly – e.g. one (1) well file may span over two (2) boxes, or one (1) box may hold twenty (20) individual files.

A typical box of well files contains:

- An average of eight (8) files

- Anywhere from 3-25 logs of varying size, with an average total combined length of 150-300 metres per box

An average file takes approximately 2-4 hours to scan in entirety (scanning time is dependent on file composition/number of logs). Older files typically take longer to digitize as they contain more logs, plus require careful handling due to age and increased document fragility.

The following table provides an overview of the types of documents that might be filed in a well file and the Commission's digitization requirements. A well file may not include every document type listed. Some files contain only a few of the document types, whereas others may hold many of those listed.

Well File Document Types	Document Size	Scanner Requirement	Blk & Wht/ Colour	DPI	Format PDF/Tiff
Well logs/Formation evaluation logs (includes Hef logs)*	Irregular *Scanned image file size cannot exceed 1 GB to support system uploading*	NeuraScanner	Colour	400	PDF/Tiff
Tour sheets	Irregular (square/slightly larger than 11x17 inch; some consist of coloured carbon copies)	Large/Wide Format Desktop	Colour Colour	400 400	PDF
Core Reports	Irregular, Letter or Legal	Desktop	Colour	400	PDF
Analyses (e.g. water, gas)	Letter	Desktop	Colour	400	PDF
Absolute Open Flow	Letter	Desktop	Colour	400	PDF
Packer Isolation tests, Pressure Volume tests	Irregular Letter or Legal	Desktop	Colour	400	PDF
Pressure Survey Test	Letter	Desktop	Colour	400	PDF
Well summary reports	Irregular, Letter or Legal	Desktop	Colour	400	PDF
Well & test hole amendments, revisions, exemptions	Irregular, Letter or Legal	Desktop	Colour	400	PDF
Work-Over/Completion reports	Irregular, Letter or Legal	Desktop	Colour	400	PDF
Drill Stem Tests/Drilling reports	Irregular, Letter or Legal	Desktop	Colour	400	PDF
Applications	Irregular, Letter or legal	Desktop	Colour	400	PDF
Approvals	Irregular, Letter or legal	Desktop	Colour	400	PDF
Geological reports	Letter	Desktop	Colour	400	PDF
Well name changes, transfers	Letter	Desktop	Colour	400	PDF
Correspondence	Letter	Desktop	Colour	400	PDF
Survey plans	Oversize (>than 12x18)	Large/Wide Format	Colour	= or > 400	PDF

**Recent well files (dating from the mid 1990's onwards) may contain one or more Hef logs. These logs can average from 350 to 750 metres in length. Hef logs are not found in "older" well files as they are produced using newer technologies. The initial contract will focus on the Commission's collection of older well files.*

4.2 Content Requirements

To respond to this RFP, Proponents are required to submit the following information:

Proponent Eligibility & Qualifications

1. Description of company eligibility.
2. Description of company qualifications and former jobs relevant to the services outlined.
3. Description of project team (number of employees, qualifications).

Location/Facility

1. Description of physical location/facility where boxes/files will be stored and scanned (may include photos).
2. Description of security measures and other protections in place to safeguard boxes/files while in the Proponent's custody and control.
3. Description of emergency response process as it applies to the management of client records.

Scanning Equipment

1. Description of scanning equipment to be used for the project (age/make/model).
2. Verification/acceptance of NeuraScanner requirement for well logs.

Proposed Approach/Processes

1. Description of end-to-end process for the receipt, preparation, scanning, restoration and return of files/file boxes to storage.
2. The number of days per week services will be performed (e.g. 5, 6).
3. Description of quality control and QA standards/processes to ensure quality and accuracy of image deliverables.
4. Description of the data transfer process (e.g. frequency, volume, schedule, etc.).
5. Description of reporting maintained to monitor/track/convey file scanning progress, box location, completed boxes, budget spend to date, etc. (include report format samples)Description of incident reporting in the event of a loss, breach or damage to Commission property and mitigation strategy.

Costing/Rates

1. Total processing cost **per file box** (includes cost for Labour).
2. Description of invoicing process for services.

Client References

1. Two client references, including organization, contact name, title, phone number, email address and date that work was performed.

4.3 Format Requirements

The following format, sequence, and instructions should be followed to provide consistency in Proponent response and ensure each proposal receives full consideration. With all pages consecutively numbered, the proposals should contain the following parts:

a) Table of contents with page numbers.

b) One-page executive summary.

c) The body of the proposal in accordance with the above content requirements. This part is not to exceed 10 pages of combined text, tables, graphics and other written presentation in support of the content requirements.

5. Evaluation

The evaluation of responses will be conducted by a team consisting of employees of the Commission. All members of the team will be bound by the same standards of confidentiality.

This section details all of the mandatory and desirable criteria against which proposals will be evaluated. Proponents should ensure that they fully respond to all criteria in order to receive full consideration during the evaluation.

The lowest priced Proposal will not necessarily be accepted. The Commission reserves the right to refuse any Proposal based on quality, service, price, reputation, experience and other criteria.

The Preferred Proponent will be the Proponent scoring the most points after evaluation. The evaluation process will consist of the following stages:

- Stage One – Mandatory Criteria
- Stage Two – Desirable Criteria
- Stage Three – Proponent Location/Facility Inspection
- Stage Four – Reference Checks (optional)

5.1 Mandatory Criteria

Proposals not clearly demonstrating that they meet the following mandatory criteria will be excluded from further consideration during the evaluation process:

- **The Proposal must be sent and received before the designated closing date and time.**
- **The Proposal must be in English and submitted electronically to** https://procurement.bcogc.ca/
- **The Proponent must confirm that any personal information received, collected or held over the course of the review will be stored and used only in Canada.**
- **The Proposal must contain an independence and objectivity statement by the Proponent.**
- **The Proposal must confirm compliance with the Commission's vaccination policy for externals/contractors.**
- **The Proponent must reside in Victoria, B.C. or Southern Vancouver Island and have a minimum of 5 years experience in digitizing paper documents.**

Failure to meet all mandatory criteria above will disqualify the Proponent's Proposal from further review.

5.2 Desirable Criteria

The Commission seeks to enter into an agreement with the Proponent who, in the opinion of the Commission, has the resources, knowledge and competence to provide the greatest value. Proposals meeting all of the mandatory criteria will be further assessed against desirable criteria.

Desirable Criteria	Weight
Proponent Qualifications	40%
Suitability of Location/Facility, Equipment & Proposed Approach	40%
Pricing: Cost per box/Rates for services	20%

5.3 Proponent Location/Facility Inspection

The Commission reserves the right to conduct an onsite inspection of the Preferred Proponent's physical location/facility to verify the information contained in the Proposal and confirm the suitability of the location and/or scanning equipment. The Commission will not enter into a contract with any Proponent whose location, facility or equipment is found to be unsatisfactory.

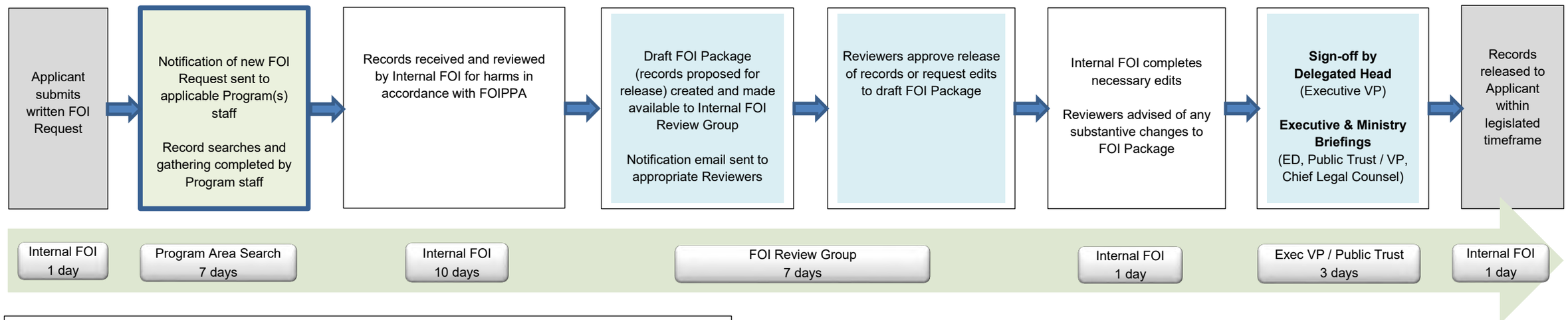
Proponent Location/Facility Criteria	Weight
Client satisfaction with Proponent location/facility and/or verification of Proposal responses	Pass/Fail

5.4 Reference Checks (Optional)

The references of the Preferred Proponent may be contacted to validate any part of their responses. The Commission reserves the right to conduct such independent reference checks or verifications as deemed necessary to clarify, test, or verify the information contained in the Proposal and confirm the suitability of the Proponent. The Commission will not enter into a contract with any Proponent whose references are found to be unsatisfactory.

Reference Check Criteria	Weight
Client satisfaction with Proponent services and/or verification of Proposal responses	Pass/Fail

INTERNAL FOI PROCESS FLOWCHART



Flowchart reflects a typical 30 business day processing timeline:

Searches for Records
- 5-7 business days are typically allocated for records searches and gathering by Commission program areas.
- If record volumes are significant, a time extension may be taken or Fee Estimate issued to the Applicant.

FOIPPA Review by Internal FOI
- 2-10 days is typically allocated for a line-by-line review of responsive records by Internal FOI staff.
- Exceptions under FOIPPA are applied to information deemed harmful to release.
- Draft FOI Package is created for review by the internal FOI Review Group.

Review & Approval by Leadership Group Members
- 5-7 business days are typically allocated for review and approval of a FOI Package by FOI Review Group.
- This time period may be increased for large and complex files if additional time is available.
- Time may be reduced if the package is small or the legislated date for response is approaching.

Sign-Off by Delegated Head (Executive VP)
- Executive sign-off occurs when: (1) any required changes to a FOI Package have been completed; and (2) all required Review Group approvals have been received.

Release to Applicant
- Requested records are released to the Applicant after required briefings have been completed.

WHAT IS FOI?

The Freedom of Information and Protection of Privacy Act (FOIPPA) enables the public to request and obtain copies of records held by government public bodies, when those records are not routinely available. These requests are known as "FOI Requests".

Who does FOIPPA apply to?

FOIPPA applies to **public bodies**, including all BC provincial government ministries, agencies, boards, commissions, and provincial Crown corporations. It also applies to local public bodies such as municipalities, regional districts, universities, hospitals, school boards and self-governing professional bodies (such as the College of Physicians and Surgeons). FOIPPA does not apply to private sector organizations in BC.

What are a public body's main obligations under FOI?

Under FOIPPA, public bodies:

- Have a legislated 30-business day time limit to respond to FOI requests, with specific exceptions which allow the ability to grant extensions of time in appropriate circumstances.
- Must consider all responsive records available to an applicant, and make every reasonable effort to assist.
- Should complete a line-by-line review of records identified as "responsive" to a request to determine whether any information contained within them requires protection from disclosure.

What oversight body ensures that FOI is done appropriately throughout government?

The Office of the Information and Privacy Commissioner (OIPC) provides independent oversight and enforcement of BC's access and privacy laws. The OIPC is responsible for monitoring how FOIPPA is administered, and is authorized to conduct investigations and audits to ensure compliance with any provision of FOIPPA. Applicants have the right to request formal review of a decision, act or failure to act with respect to a public body's administration of a FOI request under FOIPPA.

What is considered a "record" under FOIPPA?

A record is any information recorded or stored by any means, whether in physical (hardcopy) or electronic format. This includes emails, notebooks, correspondence, photographs, phone records and even information on post-it notes. If it was created in the course of your daily work, it is considered a record.

Are all requested records released under FOI?

No. Records are not automatically released to the public. There are exceptions to the public's information rights under FOIPPA. For example, an applicant will not get access to Cabinet confidences, someone else's personal information, or information that could harm another individual's business interests. An applicant will also not get access to records that could harm law enforcement, or the economic or financial interests of a public body, other individuals or the public. *See "FOIPPA Exceptions to Disclosure" for details.*

Are all requests for information handled formally?

No. Some requests for information can be satisfied informally through routine channels. Through our corporate website, the Commission makes select records information available to the public. Over time, additional information will be proactively released as the Commission works to identify information suitable for disclosure as part of its *Transparency Strategy*.

A formal FOI request is necessary when there may be sensitive or confidential information contained within a record. For example, information that:

- Was created by or relates to another government public body or its employees
- Was provided by or is about a third party (e.g. a company's financial or proprietary business information)
- Relates to government negotiation or consultative processes
- Includes personal information about an individual (e.g. landowner information, information relating to employees, etc.)

The Commission's FOI staff, in collaboration with program subject matter experts and management, identifies whether information is unsuitable for release.

What should I do if I receive a written request for information?

If a program area receives a request for a record(s) that is identified as routinely releasable (no harmful or sensitive/confidential information exists within the record), staff may provide the record to the applicant.

If the requested record(s) contains or may contain sensitive/confidential information, is not a record that's made available to the public or you are unsure, please contact the Commission's FOI Specialist, Dana Keough or send an enquiry to the FOI team inbox at FOIintake@bcogc.ca

FOI IN THE COMMISSION

The Commission receives requests for information from multiple applicants (e.g., media, interest groups) for a wide variety of subjects. During 2015-2017, 170 requests were received and processed formally under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Where records are not available through routine venues, the Commission processes requests for information internally through a formal FOI process. Over time, the Commission is looking to make more information routinely available to the public which may help to reduce the number of formal requests received.

Commission FOI "At-A-Glance"

1. **Our external website features our corporate FOI inbox (FOIintake@bcogc.ca) and information for the general public on how to submit an FOI Request**

2. **We have staff dedicated to administering FOI requests and ensuring compliance:**

   - Dana Keough (FOIPP Specialist) and Kathryn Smerechinskiy (Director)
   - It requires a "small village" to do FOI effectively. We regularly consult with the Commission's communications and legal teams, plus many of you as the subject matter experts.

3. **We are establishing a new internal FOI process that includes:**

   - A single point of contact model within each program area, where one individual receives notification of new FOI requests, coordinates records searches within their team, and ensures responsive records are supplied to the Commission's internal FOI team in a timely manner.
   - An internal FOI review group comprised of VPs/Executive Directors and Program Leads to review and approve FOI packages prior to release.
   - Formal sign-off of FOI releases by the Delegated head (CFO & Executive VP, Corporate Services).

Our "Top 3" FOI Objectives

1. To build staff awareness about FOIPPA and their accountabilities under the Act.
2. To ensure adequate and thorough searches for records are conducted.
3. To promote openness and transparency while balancing the need to protect sensitive information.

What should I do if I receive a written request for information?

If a program area receives a request for a record that's identified as routinely releasable (no harmful or sensitive/confidential information exists within the record), staff may release the record to the applicant. If the requested record appears to contain sensitive/confidential information, is not a record that's typically made available to the public or you are just unsure, please contact the Commission's FOIPP Specialist or send an enquiry to the FOI team inbox at FOIintake@bcogc.ca

HARMS ASSESSMENT CHECKLIST

A guideline for identifying potentially harmful information in FOI release materials.

Use the following "checklist" as an aid for identifying information that could potentially be harmful if released:

1. Harm to other governments

- ☐ Do the records contain confidential negotiations with other governments?
- ☐ Do the records contain information that could harm our relationship with the Canadian government, another province, a municipality or regional district, an aboriginal government or international state or states?

2. Harm to the Commission

- ☐ Could release of information be harmful to our financial interests (e.g. information has monetary value)?
- ☐ Could release of information be harmful to our economic interests (e.g. could damage the economic policies/activities for which the Commission is responsible)?
- ☐ Do the records relate to administrative or personnel management plans that are not yet public?

3. Harm to 3rd party business interests

- ☐ Do the records contain information about a business's confidential negotiations with the Commission?
- ☐ Could release of information reveal the business's trade secrets?
- ☐ Was the information supplied in confidence?
- ☐ Could release of information harm the business's competitive position, result in the Commission no longer receiving the information, or result in undue financial losses or gains?

4. Legal advice

- ☐ Do the records contain legal advice?
- ☐ Was the information intended to be confidential?
- ☐ Was the record created for the purpose of seeking or giving legal advice?
- ☐ Do the records relate to a legal matter? If yes, is the matter still ongoing?
- ☐ Are the records being used in litigation?

5. Cabinet confidences

- ☐ Were the records submitted, or prepared for submission to Cabinet/Treasury Board?
- ☐ If yes, are they draft or a final submission?
- ☐ If yes, have the records gone to Cabinet, or are they pending?
- ☐ If they've gone to Cabinet, has the information been made public? Implemented?

6. Policy advice and recommendations

- ☐ Do the records contain information that is policy advice prepared for a public body or minister?
- ☐ Do the records consist of 'draft' materials / advice / recommended courses of action?

Freedom of Information and Protection of Privacy Guidance for Contractors

The BC Energy Regulator (BCER) is required to comply with government policies and legislation related to privacy protection. In BC, our privacy protection obligations as a public body are governed by the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

FOIPPA applies to all records in the custody or control of public bodies in British Columbia.

How does FOIPPA affect a contracted service provider?

FOIPPA requires public bodies to ensure that contractors providing services on their behalf follow the same rules for collecting, using and disclosing personal information that a public body would have to follow.

Contractors must meet strict standards for protecting personal information. This is especially true when a contractor manages sensitive personal information such as health or financial information of British Columbians.

What constitutes Personal Information?

FOIPPA defines personal information as "recorded information about an identifiable individual other than contact information". Contact information typically includes information found on an individual's business card or work email signature block. Examples of **personal information** include:

- Name, residential address, personal email address or phone number
- Age, date of birth, sex, religion, race, sexual orientation, marital/family status, fingerprints
- Assigned identification numbers (SIN, drivers' license or personal health number) or symbols
- Educational, financial, criminal or employment history
- Health care history (including a physical or mental disability), medical conditions
- Personal opinions (whether true or not), but excluding those about someone else
- Patterns of behaviour captured through electronic monitoring

What are your responsibilities regarding records in your custody?

A contract may require a contractor to collect or use personal information such as a person's name, address or opinion.

As a contractor in custody of personal information, you have an obligation to take reasonable security precautions to protect it against risks, such as unauthorized access, collection, use, disclosure, or disposal.

The amount of detail in each contract relating to records management and protection of privacy will depend on the complexity of service being provided.

Records management

Records management is the system an organization uses to effectively capture and maintain information associated with business activities and transactions. Records include both print and digital records of such items as email, documents, maps and notes.

Considerations:

- What records the contractor will have to create, use or store
- Any special conditions governing the way records are managed
- Requirements about the return or disposal of records (such as maintaining a disposal log or ensuring that confidential records are shredded)

Protection of privacy

Privacy is protected by treating personal information responsibly and lawfully. This includes ensuring personal information is collected, used, and disclosed appropriately.

Considerations:

- The contractor's responsibility for the actions of its employees, agents and subcontractors
- Limits on the collection, use and disclosure of personal information *(specifications will be outlined within the contract)*
- Requirements respecting storage of personal information *(specifications will be outlined within the contract)*

Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability of that information or system.
FOIPPA requires public bodies to protect personal information by using reasonable security controls. "Reasonable" security controls means that the security arrangements are appropriate for, and proportional to, the sensitivity of the information. For example, more sensitive personal information such as

health records, should be subject to more robust security controls than less sensitive personal information, such as contact information an individual has made publicly available.

Considerations:

- Security standards - technological, physical, administrative *(specifications will be outlined within the contract)*

Access to information (Freedom of Information)

Public bodies are accountable to the public for ensuring access to records under the custody or control of the public body, with limited exceptions. This includes individuals' right of access to their personal information.

Considerations:

- Records in your custody considered to be under the control of BCER can be requested under FOIPPA. These would be records about the services you provide to BCER, not about your own operations.

  Note: In the event a request for records is received by the BCER, and it is determined that you hold records responsive to such a request, your contract manager will contact you to make appropriate arrangements. These will include instructions such as searching for records, providing original records or copies, and meeting time limits for responding.

What steps must a contractor take if they receive a request for records?

As a contracted service provider, if you receive a request from an individual or organization seeking to access records in your custody that relate to the work you have been contracted to perform on behalf of the BCER, please redirect this request to BCER immediately.

Send an email to the BCER Freedom of Information Office providing all details of the request at: FOIIntake@bc-er.ca

Information Incidents/Privacy Breaches

An information incident is an event (or series of events) involving the collection, storage, access, use, disclosure or disposal of confidential or personal information that threatens privacy or information security, and/or contravenes law or policy.

An information incident that threatens privacy is called a privacy breach and includes the theft or loss of personal information, or the access, collection, use, or disclosure of personal information that is not authorized under FOIPPA. A privacy breach may be accidental or deliberate.

The most common privacy breach happens when personal information is stolen, lost or mistakenly disclosed – for example, when a computer is stolen or when personal information is mistakenly emailed to the wrong person or distribution list.

What steps must a contractor take if a privacy breach occurs?

Contractors and service providers are required to report any suspected or actual information incidents that involve personal or business confidential information.

STEP 1: Where possible, a contractor should take immediate, common-sense steps to limit and contain a breach by **stopping the action or practice that caused or contributed to the breach**. Examples may include:

- recalling an email or recovering records
- requesting a shutdown of the system that was breached
- requesting a change in system user access permissions
- requesting a user's system or computer access be revoked
- correcting a physical security weakness (e.g. locking a location).
- Each contractor must understand what constitutes a breach of personal privacy and their role and responsibilities in the breach response process.

STEP 2: Contact BCER staff who must be aware of the incident. Send an email to the BCER Privacy Officers PrivacyOfficer@bc-er.ca and cc: Your Contract Manager.

In the event of an information incident or breach of privacy, BCER will work with you to review and assess the details of what has occurred as part of their formal Privacy Breach Response.

Freedom of Information and Protection of Privacy Guidance for Contractors

In summary, as a Contractor for the BC Energy Regulator, ensure you:

- ✓ Understand your FOIPPA responsibilities.
- ✓ Have a records management plan that supports confidentiality and security of information.
- ✓ Know who to contact if you have any questions or concerns.

For Privacy Advice and Support:

Contact the BC Energy Regulator's Privacy Officers at PrivacyOfficer@bc-er.ca.

To report an actual or suspected **Information Incident or Breach of Privacy** email PrivacyOfficer@bc-er.ca and cc your contract manager.

For Access to Information (FOI) and Records Support Contact the BC Energy Regulator's FOI support team at: FOIIntake@bcogc.ca:

Contact the BC Energy Regulator's FOI support team at: FOIIntake@bc-er.ca.

BRITISH COLUMBIA ENERGY REGULATOR

The Freedom of Information and Protection of Privacy Act (FOIPPA)

Sections of the Act / Exceptions to Disclosure

FOIPPA establishes an applicant's right to access records held by a public body. There are certain exceptions to accessing records. "Severing" is applied to records in accordance with these sections. ***Four*** *out of the 12 exceptions are mandatory (see sections are identified in red below). The other exceptions to disclosure can be applied at a public body's discretion. An organization's approach to proactive release of records should align with FOIPPA's exceptions to disclosure, as well as any other applicable legislation related to the confidentiality of information.*

Section	FOIPPA Section Title	Overview of FOIPPA Disclosure Exemptions
12	Cabinet Confidences	A provincial government public body must withhold information that would reveal Cabinet confidences (e.g. advice, recommendations, policy considerations or draft legislation/regulations submitted or prepared for submission).
13	Policy Advice, Recommendations or Draft Regulations	Covers information that would reveal advice or recommendations. This section is intended to allow for full and frank discussion of policy issues during deliberative processes.
14	Disclosure Harmful to Legal Advice	Covers communications between a public body and its legal counsel (protects solicitor client privilege).
15	Disclosure Harmful to Law Enforcement	Covers information that would harm a law enforcement matter.
16	Disclosure Harmful to Intergovernmental Relations or Negotiations	Covers matters which could harm the relations between BC's levels of government and governments from other provinces and jurisdictions (e.g. Government of Canada/Province of Canada, council of municipality, regional district board, aboriginal government, government of a foreign state, international organization of states).
17	Disclosure Harmful to Financial or Economic Harm	Covers information which, if released, would cause financial or economic harm to the public body or to the government.
18	Disclosure Harmful to Conservation of Heritage Sites	Covers information about heritage sites which would result in the exploitation, damage of, or interference with the conservation of those sites. This includes: fossil sites or anthropological sites; an endangered, threatened or vulnerable species (plants, vertebrates, invertebrates); and rare or endangered living resources.
18.1	Disclosure Harmful to Interests of an Indigenous People	Covers information that could reasonably be expected to harm the rights of an Indigenous people to maintain, control, protect or develop their cultural heritage, traditional knowledge, traditional cultural expressions, or manifestations of sciences, technologies or cultures.
19	Disclosure Harmful to Individual or Public Safety	Covers information that could result in harm to any person's safety, mental, physical or emotional health or to public safety.
20	Information That Will Be Published or Released Within 60 Days	A public body may withhold information from an applicant if it is already for sale to the public, or if the public body plans to release or publish the information within 60 days.

21	Disclosure Harmful to Business Interests of a Third Party	Public bodies are often in possession of commercial, financial, scientific or technical information of third party's and must withhold that information from an applicant if releasing it would cause harm to the business. A specific three-part test must be met in order to appropriately apply the section.
22	Disclosure Harmful to Personal Privacy	Personal information belongs to that individual and must not be disclosed if it would be an unreasonable invasion of privacy. Except in very limited circumstances, public bodies must not release an individual's information to anyone else without their consent.

BRITISH COLUMBIA ENERGY REGULATOR

HARMS ASSESSMENT CHECKLIST

Guideline for Identifying Potentially Harmful Information in FOI Release Materials

Use the following "checklist" as an aid for identifying information that could potentially be harmful if released:

1. **Harm to Other Governments**
   - ☐ Do the records contain confidential negotiations with other governments?
   - ☐ Do the records contain information that could harm our relationship with the Canadian government, another province, a municipality or regional district, an aboriginal government or international state or states?

2. **Harm to the BCER**
   - ☐ Could release of information be harmful to our financial interests (e.g. information has monetary value?)
   - ☐ Could release of information be harmful to our economic interests (e.g. could damage the economic policies/activities for which the BCER is responsible)?
   - ☐ Do the records relate to administrative or personnel management plans that are not yet public?

3. **Harm to 3rd Party Business Interests**
   - ☐ Do the records contain information about a business's confidential negotiations with the BCER?
   - ☐ Could release of information reveal the business's trade secrets?
   - ☐ Was the information supplied in confidence?
   - ☐ Could release of information harm the business's competitive position, result in the BCER no longer receiving the information, or result in undue financial losses or gains?

4. **Legal Advice**
   - ☐ Do the records contain legal advice?
   - ☐ Was the information intended to be confidential?
   - ☐ Was the record created for the purpose of seeking or giving legal advice?
   - ☐ Do the records relate to a legal matter? If yes, is the matter still ongoing?
   - ☐ Are the records being used in litigation?

5. **Cabinet Confidences**
   - ☐ Were the records submitted, or prepared for submission to Cabinet/Treasury Board?
   - ☐ If yes, are they draft or a final submission?
   - ☐ If yes, have the records gone to Cabinet, or are they pending?
   - ☐ If they've gone to Cabinet, has the information been made public? Implemented?

6. **Policy Advice and Recommendations**
   - ☐ Do the records contain information that is policy advice prepared for a public body or minister?
   - ☐ Do the records consist of 'draft' materials / advice / recommended courses of action?

BRITISH COLUMBIA ENERGY REGULATOR

SEARCH CHECKLIST

Guideline for Completing a Search for Responsive Records

Use the following "checklist" as an aid for identifying areas for searching and locating records:

1. **Outlook**
   - ☐ Outlook email box (including inbox, sent, deleted, and archived folders)
   - ☐ Shared outlook email boxes

2. **Shared/Personal Drives**
   - ☐ K: Drive (or others)
   - ☐ F: Drive
   - ☐ OneDrive
   - ☐ SharePoint Sites
   - ☐ Personal PC or hard drive

3. **Hardcopy Records**
   - ☐ Hardcopy files (other than those kept in the FSJ Records Centre or Offsite Storage)
   - ☐ Notebooks
   - ☐ Other hardcopy records

4. **Databases and Information Systems**
   - ☐ Kermit
   - ☐ IRIS
   - ☐ AMS Application
   - ☐ AMS Review (CRD)
   - ☐ CMIS
   - ☐ GIS and Spatial Data
   - ☐ Other database or information systems

Employee Signature Confirming Search:_____

From: FOI Intake
Subject: CALL FOR RECORDS: BCER-20XX-XXX (Brief Description)

Good afternoon,

The BCER has received the following new FOI request (Applicant type: Choose an item.):

Description of Request

Please forward all responsive records to: FOIIntake@bc-er.ca or directly to me by**:** **Date**. If you do not have responsive records, please indicate this by a reply to this email.

Provide any other relevant details.

If you believe this Call for Records should be directed to another BCER employee or program area, please advise.

Thank you.

From: FOI Intake
Subject: FOR REVIEW & APPROVAL: BCER-20XX-XXX (Brief Description)

Good afternoon,

FOI package **BCER-20XX-XXX** is ready for your review and approval. Please see the attached redline package (attach package or link to materials)

Note to Reviewers:

- Please refer to the attached **FOI Release Approval Form** for request details.
- ADD ANY OTHER RELEVANT DETAILS.

Please reply with your approval or comments by: Date.

If you have any questions, please let me know.

Thank you.

From: FOI Intake
Subject: FOR SIGN-OFF: BCER-20XX-XXX (Brief Description)

Good afternoon,

FOI request **BCER-20XX-XXX** is ready for your review and sign-off. Please see the attached FOI Release Approval Form for the request details.

Approvals have been received from: (ENTER APPROVERS NAMES).
ADD ANY OTHER RELEVANT INFORMATION.

To approve release, please add your electronic signature to the approval form. Your response would be appreciated by: **[DATE]**

If you have questions, please let me know.

From: FOI Intake
To:
Subject: [Name of Public Body] Consultation - BCER-[Request #] - Due: [Date]

Hello [Name of Public Body],

Re: Request for Consultation – *Freedom of Information and Protection of Privacy Act* (FOIPPA)

The BC Energy Regulator has received a request for information from a [applicant type] applicant:

[description of request]

The attached records gathered in response to the request, originated from or concern your agency and we would like to get the [public body's acronym] views and recommendations on disclosure. In order to meet our legislated due, we would appreciate your written response by: [due date]; however, if you do not respond back by this date, we will proceed with processing the request and release in accordance with FOIPPA. For your convenience, a copy of FOIPPA can be found online: Freedom of Information and Protection of Privacy Act (gov.bc.ca)

Please forward your written response to: FOIIntake@bc-er.ca.

Thank you,
Kind regards,

BRITISH COLUMBIA ENERGY REGULATOR

FOI Release Approval Form
Request: 292-30/
BCER-20XX-XXX

Overview of Request, Harms & Release Recommendations

Request Received: Enter Date **Legislated Due Date:** Enter Date **Applicant Type:** Select

Description*:* Includes wording of information request received from applicant

Comments/Background:

- Includes details on what program areas were canvassed and who responsive records were received from.
- Includes summary of severing recommendations applied to address concerns (sections of FOIPPA applied and high-level rationale).

Consultations:

- Includes details on any 3rd parties consulted (e.g. ministries, industry, etc.)
- Includes high level summary of 3rd party responses.
- Identifies whether severing any severing was applied to address concerns.

Release Recommendation: ☐ Full disclosure ☐ Partial disclosure ☐ Access denied ☐ Phased release

Website Publication Recommendation: ☐ **Suitable** for publication ☐ **Not Recommended** for publication
(When not recommended for publication, include the following exemption statement to provide rationale) This request is not recommended for publication because the records for release include: (choose applicable exemption and remove all others)

- ❖ *Personal Information or information that could lead to the identification of the Applicant or other persons.*
- ❖ *Information that may harm relations with a First Nation.*
- ❖ *Information that may harm relations with another government.*
- ❖ *Information that may harm a third party's business interests.*
- ❖ *Information that is not suitable for proactive disclosure based on a formal risk assessment that disclosure to the public may threaten the safety of a person or harm the security of any property or system.*

Specialist, FOIPP & IM: Dana Keough	Signature:	Date: Click here to enter a date
Director, Records & IM: Mahia Frost	Signature:	Date: Click here to enter a date.

Executive Sign-Off - Agreement with Recommendations

EVP, People, Reconciliation & Transformation: Sara Dickinson	Signature:	Date: Click here to enter a date.

BRITISH COLUMBIA ENERGY REGULATOR

Your File:
Our File: BCER-20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and address]

Dear [**Name]:

Thank you for consulting with the BC Energy Regulator (BCER) on the release of records relating to:

[**details of consultation request]

The BCER recommends partial disclosure pursuant to [**applicable sections] of FOIPPA as shown on the attached records in redline boxes. The recommended redactions are shown on the attached redline. Please note that we have only provided recommendations for those records that concern the BC Energy Regulator and have not made any further comment on records related to any third party or other government agencies.

If you have any questions, please contact: FOIIntake@bcer.ca

Sincerely,

[**Signature]
BC Energy Regulator

Physical/Courier/Mailing
6534 100 Avenue
Fort St. John, BC V1J 8C5

T: 250.794.5200
F: 250.794.5390

www.bc-er.ca

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Confirmation
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) received your request for information under FOIPPA for:

["Description of request"]

We will make every effort to provide the information available to you under FOIPPA as quickly as possible. FOIPPA allows 30 business days for us to respond to your request; therefore, we will be responding on or before [**Date].

However, you should also be aware that the Act does allow, in limited circumstances, for the 30-day time period to be extended and for fees to be charged. We will notify you as soon as possible if there will be a requirement to extend the time limit for responding to your request or to charge fees.

If you have any questions now or during the processing of your request, please contact the BCER at: FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Fee Estimate
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) received your request for **[*"Summary of request"].***

Section 75 of FOIPPA provides that we may charge a fee for certain limited costs of providing you with the requested information as outlined below. The fee for providing the records is estimated to be **$*****.

Searching & locating relevant records	
15 minutes/1" file @ $30/hour:	$***
Scanning records	
# of pages @ $0.10/page	
# of large format pages @ $4/page	$***
Preparing records for disclosure	
# Hours @ $30/hour	$***
Shipping (if applicable)	$***
Total:	$***
Deposit Required:	**$*** **

Please note that you must provide the BCER with a cheque or money order representing the deposit for the above services in the amount of [$XXX] before we will continue processing your request. Kindly make this cheque payable to the Minister of Finance and return to my attention at:

BC Energy Regulator
6534 100th Avenue
Fort St John BC V1J 8C5

This is an estimate of the specific costs associated with processing your request. All reasonable efforts have been made to generate an accurate estimate; however, you will be required to pay the actual cost whether it is higher or lower than the estimate. We will inform you if it is determined that the actual

cost will exceed the estimate prior to providing any further service. Should the final costs be less than the above quoted total, the balance will be adjusted accordingly.

FOIPPA provides that we may excuse you from paying all or part of the fee if you cannot afford to pay, or if the records relate to a matter of public interest. If you wish to request a fee waiver, please provide us with written detailed reasons why a fee waiver should apply. Once we have reviewed your submission, we will notify you of our decision. While FOIPPA imposes an obligation on us to respond to your request within 30 days, the time period that elapses while we await your deposit will not be included in the calculation of your response time. If we do not here from you by [**Date], we will consider the file closed.

You may ask the Office of the Information and Privacy Commissioner (OIPC) to review this fee estimate. FOIPPA allows you 30 days from the date of this letter to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038, Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting the review. Please contact the BCER at FOIIntake@bc-er.ca with any questions or concerns regarding this fee estimate.

Sincerely,

[**Signature**]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice to Third Party – Request for Consultation
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) has received a request under FOIPPA to disclose records that may affect the business interests of your company [***describe records as they relate to the third party].

The attached records have been reviewed by the BCER and we have determined that the records contain information that might be harmful to your business interests. You may be able to provide us with additional information from your business' perspective that would help us to determine whether disclosure of these records could result in significant harm. For your convenience, I have attached an explanation of Section 21 of FOIPPA. After reviewing the attached material, please provide your views on its disclosure in writing to me by [**date].

You may:

1. Consent to the disclosure of the information,
2. Request that the BCER remove portions of the information, while disclosing the remainder, by providing us written representations as to why the information should be withheld, or
3. Make written representations explaining why you feel the records or information should not be disclosed.

The BCER must disclose the information to the applicant unless it can be shown that the records contain certain types of information (described in more detail on the attached explanatory note); the information was supplied in confidence; and the disclosure of the information could reasonably be expected to result in one of more of the harms as specified. If you wish to have any of the information pertaining to your business withheld, it is important that you provide clear and specific reasons. In your submission, please focus on the type of harm directly related to Section 21, as specified in the attachments. Your input will be considered, along with other relevant factors, in deciding whether to disclose the records. Please note if we do not receive written representations from you by the date indicated above, we are still required under FOIPPA to make a decision based on the information we have available. We will write to you by [***date] to inform you of the BCER's decision on the release of this information.

For any questions or further clarification, please contact the BCER at: FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

Physical/Courier
6534 100 Avenue
Fort St. John, BC VIJ 8C5

Mailing
Bag 2
Fort St. John, BC V1J 2B0

T: 250.794.5200
F: 250.794.5390

www.bc-er.ca

EXPLANATORY NOTE
THIRD PARTY BUSINESS INTERESTS

Purpose of the *Freedom of Information and Protection of Privacy Act* (FOIPPA)

The *Freedom of Information and Protection of Privacy Act* balances the public's right of access to public bodies' records with the need to protect from disclosure information which would harm the interests of the public body or a third party. When a request is made for access to records, we are required to provide access to as much of the requested information as possible and may only withhold information covered by the specific exceptions provided by FOIPPA.

Request for Information which May Affect your Business Interests

We have received a request for access to records which contain information relating to your business. Section 21 of FOIPPA provides for exception to the right of access when disclosure of the information results in significant harm to a third-party's business interests. Under Section 21, the head of a public body must withhold access to the information if the information satisfies all three parts of the test set out below:

1. The information is a trade secret or commercial, financial, labour relations, scientific or technical information of the third party; **AND**
2. The information was supplied, implicitly or explicitly, in confidence. There must be evidence that the information has been consistently treated in a confidential manner; **AND**
3. One or more of the following harms will occur if the information is disclosed.
   The disclosure of the information will:
   - Harm significantly the competitive position or interfere significantly with the contractual or other negotiations of the third-party.
   - Result in similar information no longer being supplied to the BCER where it is in the public interest that similar information continues to be supplied. This does not apply where a statute or regulation requires that the information be supplied.
   - Result in undue loss or gain to any person or organization.
   - Reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

Opportunity for Input

The BCER is sending you notice of this request to give you opportunity to consent to the release or express any concerns you may have regarding the disclosure of the third-party information related to your business. Your input would be valuable in helping the Commission make an informed decision on disclosing the records.

You may respond to this notice by:

1. Consenting in writing to the disclosure of all or portions of the information; or
2. Making written representations to the BCER explaining why disclosure of the information would be harmful to your business interests.

Written Representations

If you choose to make written representations, your representations will be one of the factors that the BCER considers in deciding whether to disclose the requested information. Your reasons should be clear and as specific as possible to help the BCER decide whether the records can be disclosed. Please include detailed, factual, and objective evidence that will assist us to answer the following questions:

- Is the information a trade secret? Is it financial, commercial, labour relations, scientific or technical information?
- Was the information in your view supplied to the BCER in confidence?
- Can the release of the information reasonably be expected to cause one or more of the harms listed above?

In making your representations:

- Direct your comments only to the question of whether the specified information that relates to your business interests should or should not be disclosed.
- Identify the exact portions of the records that you wish us to withhold. (You may highlight information on the electronic copies that you feel should not be disclosed.)

Notification of Decision and Right of Appeal

The BCER will consider your representations in deciding on disclosure of the requested information. If we decide to disclose all or some of the information, we will notify you before the information is disclosed so that you may have an opportunity to request a review of the decision. Under Section 52 of FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review the decision of the BCER regarding the release of this information. You have 20 days from the receipt of the BCER's decision to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Facsimile: 250.387.1696
Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with your contact information along with copies of your written representations, the BCER's decision letter; and the reasons or grounds upon which you are requesting the review.

Detailed information on requesting a review can be found on the OIPC's website: https://www.oipc.bc.ca/

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Additional Time Extension
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request for access to records relating to **[**summary of request**].**

My letter of [**first extension date] advised that the BCER required a 30-day extension in order to process your request. Further to this, and to allow the BCER time to complete the consultation process; we have requested and received and additional **XX**-day extension from the Office of the Information and Privacy Commissioner of BC (OIPC) under section **[quote section 10(1)(b)(c)(d)]** of FOIPPA. Our due date will now be [**Date]. We will make every attempt to provide this information to you sooner if possible.

If you feel this time extension is unjustified, you may ask the OIPC to review this decision. You have 30 days from receipt of this notice to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you wish to request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting the review. Please contact FOIIntake@bc-er.ca if you have any questions.

Sincerely,

[**Signature**]
BC Energy Regulator

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Notice of Decision Subsection 24
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) has reached a decision regarding your request for information under FOIPPA.

After considering all relevant factors, including the representations received from the third party whose interests could be affected by disclosure, the BCER has decided to grant access to the records.

The third party has 20 days to request the Information and Privacy Commissioner review this decision. If the third party does not request a review, we will provide you access to the records on [**Date].

Please write FOIIntake@bc-er.ca if you have any questions or require any further clarification.

Sincerely,

[**Signature**]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Notice of Decision
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) has reached a decision regarding your request for information under FOIPPA. After considering all relevant factors, including the representations received from the third party whose interests could be affected by disclosure, the BCER has decided to refuse access to the records based on [**insert specific sections of FOIPPA]. A complete copy of the Act is available online at: Freedom of Information and Protection of Privacy Act (gov.bc.ca)

Under Section 52 of FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review this decision. You have 30 days from receipt of this notice to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038, Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you wish to request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting a review. Please write FOIIntake@bc-er.ca if you have any questions regarding this decision or require further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Third-Party Review
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

The BC Energy Regulator (BCER) herby gives notice that the processing of your request for access to information has been delayed by a review by the Office of the Information and Privacy Commissioner (OIPC). The review was requested by a third party who has an interest in the requested information.

The records you have requested contain information that may harm the business interests of the third party if disclosed. For further information regarding your rights during this review, please contact:

Information & Privacy Commissioner for BC
PO 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

The BCER will resume processing your request as soon as the OIPC has made a decision in relation to the review requested by the third party. If you have any questions regarding this delay, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Third-Party Consultation Subsection 23(4)
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing regarding your request for access to records held by the BC Energy Regulator (BCER).

The requested records contain information that may affect the interests of another business, pursuant to Section 21(1) of FOIPPA. To assist us in determining whether we may disclose this information, we are giving that third party an opportunity to make written representations concerning the disclosure. FOIPPA allows 30 business days from the date of this notice; therefore, we will notify you of our decision regarding the disclosure of the records by [**date].

Consultation will allow the BCER to provide you with a complete response to your request. If you have any questions, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER-20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Notice of Time Extension
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request for access to records relating to [**brief summary of request].

The BCER normally responds to requests for information within 30 days after receiving the request; however, in limited circumstances FOIPPA provides that we may extend this time limit when necessary. We are extending the response date by an additional 30 days under Section 10(1)(**a, b or c) [**quote section]. This will enable the BCER to provide you with a complete response by [**date].

If you feel this time extension is unjustified, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review this decision within 30 days from receipt of this notice by writing to:

Information & Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Telephone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you wish to request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting the review. If you have any questions regarding this time extension, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Decision for Fee Waiver Request
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing in response to your letter requesting a waiver of the fees estimated in response to your request for [**brief summary of request**].

We have fully assessed your request and [**decision and reasoning**].

You may ask the Office of the Information and Privacy Commissioner (OIPC) to review our decision to [**accept or decline**] your request to waive the fees related to your request. FOIPPA allows you 30 days from the date of this letter to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you wish to request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting the review. Please write FOIIntake@bc-er.ca if you have any questions regarding this decision or require further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Decision Subsection 23(3)
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

Thank you for your views on the disclosure of [**describe requested records as they relate to third party]. The BC Energy Regulator (BCER) is writing to inform you of its decision.

After considering all relevant factors, including your representations on why these records should not be disclosed, the BCER has decided to grant the applicant access to these records. Our decision is based on the following: [**insert explanation of why Section 21 or 22 does not apply].

Under Section 24 of FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review the decision to disclose these records. You have 20 days from the date of this notice to request a review by writing to:

Information & Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If no request for review is made within 20 days, the applicant will be given access to the records. Please write FOIIntake@bc-er.ca if you have questions regarding the BCER's decision or require further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Decision
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

Thank you for your views on the disclosure of [**describe requested records as they relate to third party]. After considering your representations on why these records should not be disclosed and all other relevant factors, the BC Energy Regulator has decided to refuse the applicant access to these records. This decision is based on [**insert specific sections of FOIPPA].

The applicant has the right to ask the Office of the Information and Privacy Commissioner (OIPC) to review this decision.

If you have any further questions or concerns, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Notice of Receipt of Transferred Request
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

Your request for: **[**Details of request]** was transferred from [**name of public body] under Section 11 of FOIPPA to the BC Energy Regulator (BCER). It was transferred because {[**choose one of more of the following] the responsive records were produced by or for the BCER, the BCER was the first to obtain the records, or the records are in the custody or under the control of the BCER}.

FOIPPA allows 30 business days for us to respond to your request; therefore, we will respond on or before [**date]. We will make every effort to respond sooner if possible; however, you should also be aware that the Act does allow, in limited circumstances, for the 30-day time period to be extended and for fees to be charged. We will notify you as soon as possible if there is a requirement to extend the time limit for responding to your request or to charge fees.

If you have any questions, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

Physical/Courier/Mailing
6534 100 Avenue
Fort St. John, BC V1J 8C5

T: 250.794.5200
F: 250.794.5390

www.bc-er.ca

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – Response
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request for access to records relating to [**brief description of records].

Please be advised that in accordance with Section [**section #] of FOIPPA, the BCER is unable to disclose the requested records. The information is excepted from disclosure under Section [**quote section]. A complete copy of FOIPPA is available online at: Freedom of Information and Protection of Privacy Act (gov.bc.ca)

Pursuant to section 52 of FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request. You have 30 business days from the date of this letter to request a review by writing to:

Information & Privacy Commissioner of BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with a copy of this letter, a copy of your original request and the reasons or grounds upon which you are requesting the review. Please write FOIIntake@bc-er.ca if you have any questions regarding your request or require any further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER-XXXX-XX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name & Address]

Dear [Salutation]:

Re: Request for Access to Records – Response
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request for access to records relating to ***[**Brief description of request]***

Please find attached an electronic copy of the records located in response to your request. **OR** The records located in response to your request will be delivered through the BCER's secure file transfer site Web Transfer Client (bc-er.ca). Your access credentials will be provided to you in a separate self-destructing message. The records will be available for 14 days from the date of this letter; therefore, it is recommended you download or transfer files to your desired personal location.

[**Use website publication note, if applicable] Please note, a copy of these records will be published on the BCER's website within a minimum of five business days after release. To find out more about proactive disclosure of requests, please access the BCER website: BC Energy Regulator (bc-er.ca). Your file is now closed. Pursuant to section 52 of the FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA within 30 business days by writing to:

Information and Privacy Commissioner
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response, and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process can be found on the OIPC website: https://www.oipc.bc.ca. Please write FOIIntake@bc-er.ca, if you have any questions regarding your request or require any further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and Address]

Dear [**Salutation]:

Re: Request for Access to Records – No Records Located
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request received by the BC Energy Regulator (BCER) for: ***[** summary of request].*** Although a thorough search was conducted, no records were located in response to your request. Your file is now closed.

Pursuant to section 52 of FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA. Please note that you have 30 business days to file your review with the OIPC by writing to:

Information and Privacy Commissioner for BC
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response and any other related correspondence; and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process, can be found on the OIPC website: https://www.oipc.bc.ca. If you have any questions regarding your request or require any further clarification, please write FOIIntake@bc-er.ca.

Sincerely,

[**Signature]
BC Energy Regulator

File: 292-30/BCER20XX-XXX

[**Date]

VIA ELECTRONIC MAIL: [email address]**

[**Name and address]

Dear [Salutation]:

Re: Request for Access to Records – Response
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further regarding your request for access to records relating to ***[**details of request].***

The records located in response to your request [are attached **[OR]** will be delivered through the BCER's secure file transfer site: Web Transfer Client (bc-er.ca). Your access credentials will be provided in a separate self-destructing message. The records will be available for 14 days from the date of this letter; therefore, it is recommended that you download or transfer files to your desired personal location.] Some information has been withheld pursuant to section(s): ***[**list applicable sections].*** A complete copy of FOIPPA is available online at: Freedom of Information and Protection of Privacy Act (gov.bc.ca).

[Use website publication note if applicable]**: Please note, a copy of these records will be published on the BCER's website within five business days after release. To find out more about proactive disclosure of requests, please access the BCER website: foi-proactive-disclosure-policy.pdf (bc-er.ca). Your file is now closed. Pursuant to section 52 of the FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA within 30 business days by writing to:

Information and Privacy Commissioner
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street
Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696 Email: info@oipc.bc.ca

If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response, and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process can be found on the OIPC website: https://www.oipc.bc.ca. Please write FOIIntake@bc-er.ca, if you have any questions regarding your request or require any further clarification.

Sincerely,

[**Signature]
BC Energy Regulator

OFFICE OF THE
INFORMATION &
PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Time Extension Application Form – section 10(1)(d)

***Freedom of Information and Protection of Privacy Act* (FIPPA)**

Note: *This form is for any time extension application under section 10(2)(a) based on:*

- *section 10(1)(d) consent*

Please attach written proof of the applicant's consent.

Please submit this form **at least 3 business days** before the due date, and ensure that all information is complete and accurate.

Section 1 – Public body background *(required: all fields)*

OIPC file # of previous extension (if applicable):

Public body (full name): BC Energy Regulator
Public body File #:
Public body Contact Name: Dana Keough
Contact Direct Line: 250-794-5295
Contact Email Address: Dana.Keough@bc-er.ca

Please provide a brief description of the original request:

Date request for records received (m/d/yyyy):
Original due date of request (m/d/yyyy):

Was a fee estimate sent? ❒Yes ■No
Date fee estimate sent (m/d/yyyy):
Date deposit or full fee paid (m/d/yyyy):
Date of fee waiver decision (m/d/yyyy):

Current request due date (m/d/yyyy):
Number of business days requested for this extension:
Proposed due date (m/d/yyyy):

Has the public body already taken a time extension under section 10(1)?

■ Yes ❒ No

If so, please indicate:

Date of time extension (m/d/yyyy):

Number of days extended:

Basis for time extension:

❒s. 10(1)(a) ❒s. 10(1)(b) ❒s. 10(1)(c) ❒s. 10(1)(d)

Date of letter notifying applicant of the extension (m/dd/yyyy):

Has the applicant complained to the OIPC about this time extension?

❒Yes ■No

Section 2 – Proof of applicant consent *(required: attachment)*

*Please **attach** written proof of the applicant's consent to the time extension. Emails are an acceptable form of proof.*

Forms missing proof of applicant's consent will not be processed.

(Please refer to page 9 of the Time extension guidelines for public bodies for more information.)

Click to

Submit Form

OFFICE OF THE
INFORMATION &
PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Time Extension Application Form – First Request

***Freedom of Information and Protection of Privacy Act* (FIPPA)**

Note: *This form is for time extension applications to the OIPC:*

Under section 10(2)(a) based on:
- *section 10(1)(a) insufficient detail*
- *section 10(1)(b) large volume*
- *section 10(1)(c) consultation*

Under section 10(2)(b):
- *If the commissioner otherwise considers that it is fair and reasonable to extend the time for responding*

Do not use this form for applications based on section 10(1)(d) consent.

Please submit this form **at least 3 business days** before the due date, and ensure that all information is complete and accurate.

Section 1 – Public body background *(required: all fields)*

Public body (full name): BC Energy Regulator
Public body File #:
Public body Contact Name: Dana Keough
Contact Direct Line: 250-795-5295
Contact Email Address: Dana.Keough@bc-er.ca

Please provide a brief description of the original request:

Date request received (m/d/yyyy):
Original due date of request (m/d/yyyy):

Was a fee estimate sent? ❒Yes ■No

If yes,
Date fee estimate sent (m/d/yyyy):
Date deposit or full fee paid (m/d/yyyy):
Date of fee waiver decision (m/d/yyyy):

Current request due date (m/d/yyyy):
Number of business days requested for this extension:
Proposed due date (m/d/yyyy):

Has the public body already taken a time extension under section 10(1)?

■ Yes ❒ No

If so, please indicate:

Date of time extension (m/d/yyyy):

Number of days extended:

Basis for previous time extension:

❒ s. 10(1)(a) ❒s. 10(1)(b) ❒s. 10(1)(c) ❒ s. 10(1)(d)

Date of letter notifying applicant of the extension (m/d/yyyy):

Has the applicant complained to the OIPC about this time extension?

❒ Yes ■No

Section 2 - Grounds for Current Extension Application *(required: choose all that apply)*

❒ **Section 10(2)(a)**

- ❒ s. 10(1)(a) (insufficient detail)
- ❒ s. 10(1)(b) (volume of records)
- ❒ s. 10(1)(c) (consultation)

❒ **Section 10(2)(b)**

Section 3 – Additional information (*required for each selection made in section 2)*

10(1)(a) Insufficient detail *(required: all fields)*

Please include the following with your submission:

- A complete copy of the original request.

Explain how the original request does not provide sufficient detail:

Explain why satisfactory clarification from the applicant was not obtained within 60 business days (or 30 business days if the public body's own time extension was not taken):

10(1)(b) Volume of records *(required: either volume of records requested or volume of records searched or both, and an explanation regarding unreasonable interference).*
(Please refer to pages 6-7 of the Time extension guidelines for public bodies for more information)

LARGE VOLUME OF RECORDS REQUESTED
Approximate number of pages of responsive records:

LARGE VOLUME OF RECORDS SEARCHED
Number of pages searched:
Number of program areas searched:
Total amount of time spent performing search:

UNREASONABLE INTERFERENCE WITH THE OPERATIONS OF THE PUBLIC BODY
Explain how meeting the time limit would unreasonably interfere with the operations of the public body:

Current status
Please describe the current status of processing this request and any other relevant information:

10(1)(c) Time for consultation *(required: all fields, for each public body/third party consulted)*
(Please refer to page 8 of the Time extension guidelines for public bodies for more information)
Full name of the public body or third party:
Number of pages sent or to be sent for consultation:
Date consultation was sent or will be sent (m/d/yyyy):
Why is consultation necessary to make a decision about access:

What is the third party or public body's interest in the record:

Current status of the consultation, including efforts made to obtain a response to the consultation and expected return date (m/d/yyyy):

10(2)(b) *(required: circumstances and explanation) (See pages 9-10 of the time extension guidelines. Please note the need for exceptional circumstances, such as forest fires, flooding, court involvement, and unforeseeable issues)*

Explain why it would be fair and reasonable for the Commissioner to grant a time extension. Include a chronology of the processing of the request and an explanation for any delays:

Section 4 – Additional comments

Please provide any additional comments or details that will assist in the decision on this request:

Click to

Submit Form

BRITISH COLUMBIA ENERGY REGULATOR

Additional External Resources Used by the BCER

Table of Contents - Freedom of Information and Protection of Privacy Act (gov.bc.ca)

FOIPPA Policy & Procedures Manual - Province of British Columbia (gov.bc.ca)

Records Management Guides and Learning - Province of British Columbia (gov.bc.ca)

Records Management - Province of British Columbia (gov.bc.ca)

Privacy & Personal Information in the Public Sector - Province of British Columbia (gov.bc.ca)

FOIPPA Foundations (mytrainingbc.ca)

Administrative Records Classification System - Province of British Columbia (gov.bc.ca)

Guidance Documents – Office of the Information and Privacy Commissioner for BC (oipc.bc.ca)

BRITISH COLUMBIA ENERGY REGULATOR

File: 292-30/BCER-2023-017

December 18, 2023

VIA ELECTRONIC MAIL:

Dear :

Re: Request for Access to Records – Response
***Freedom of Information and Protection of Privacy Act* (FOIPPA)**

I am writing further to your request received by the BC Energy Regulator (BCER) for copies of:

1. **Current organizational charts that indicate freedom of information personnel and information management personnel**
2. **Delegation of authority charts for FOIPPA**
3. **Policies or procedures regarding freedom of information (not privacy), including policies and procedures regarding the routine release of information and proactive disclosure.**
4. **Final reports regarding the public body's performance reporting, program evaluations, or project implementation plans or reviews with respect to freedom of information.**

The records located in response to your request will be delivered through the BCER's secure file transfer service site. Your user credentials will be provided in a separate email. Please note, the password provided is temporary and you will be prompted to change it upon first log in. Your account will be active and the record package accessible for 30 days after which your account will expire, and the records will be deleted. It is recommended you download or transfer files to your desired personal location.

A copy of these records will be published on the BCER's website within a minimum of ten business days after release. To find out more about proactive disclosure of requests, please access the BCER website: BC Energy Regulator (bc-er.ca). Your file is now closed.

Pursuant to section 52 of the FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA. **Please note that you have 30 business days to file your review with the OIPC by writing to:**

Information and Privacy Commissioner
PO Box 9038 Stn Prov Govt
4th Floor, 947 Fort Street

Victoria BC V8W 9A4
Phone: 250.387.5629 Fax: 250.387.1696
Email: info@oipc.bc.ca

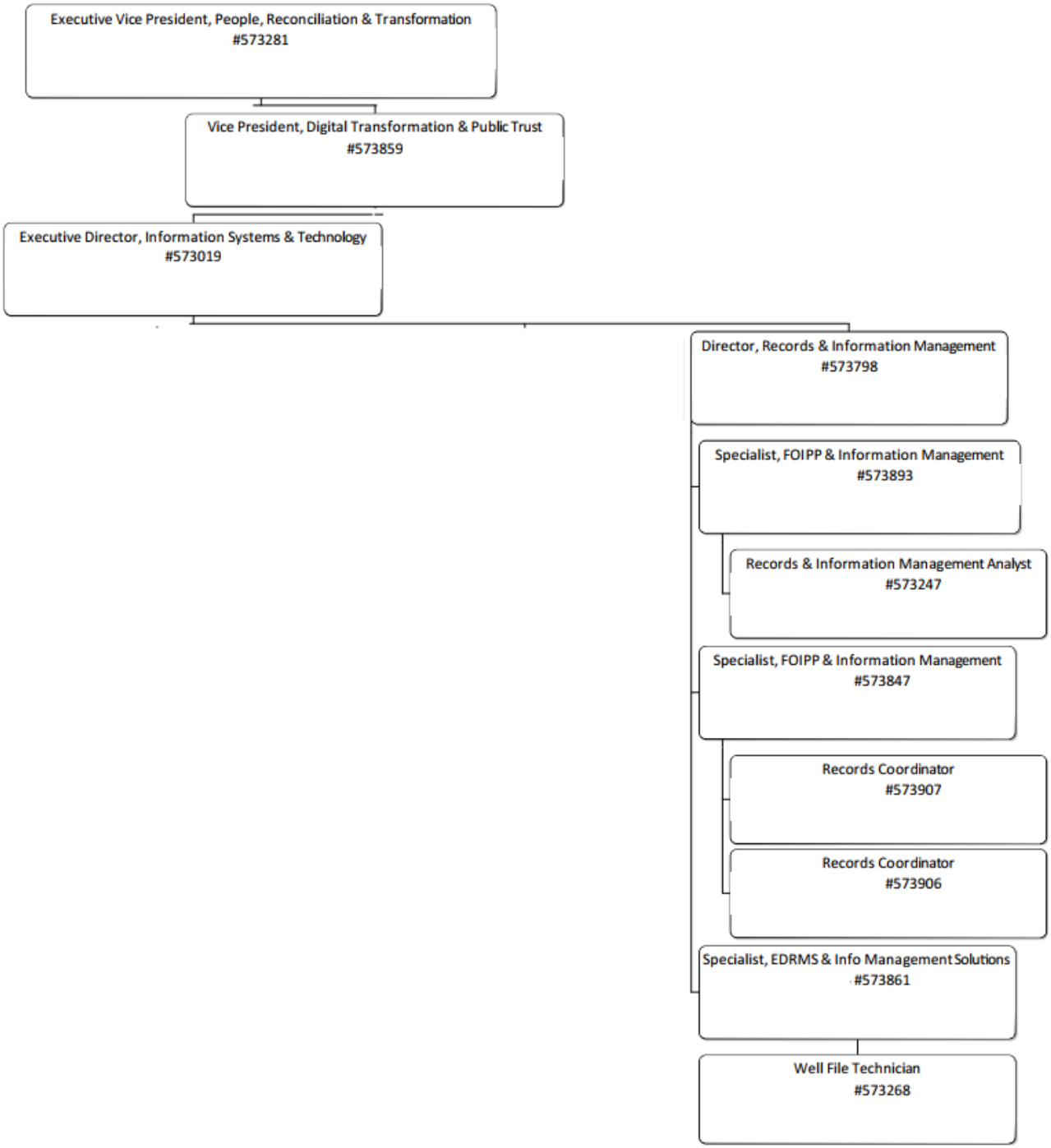
If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response, and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process can be found on the OIPC website: https://www.oipc.bc.ca. Please write FOIIntake@bc-er.ca, if you have any questions regarding your request or require any further clarification.

Sincerely,

D. Keough
BC Energy Regulator

BRITISH COLUMBIA **ENERGY REGULATOR**

Records & Information Services Branch



Delegation of duties, powers and functions of the head of the public body under the *Freedom of Information and Protection of Privacy Act* – Broader Public Sector

BEFORE YOU BEGIN

This delegation instrument template is designed to assist public bodies in the broader public sector in British Columbia in delegating duties, powers or functions of the head of the public body under section 66 of the *Freedom of Information and Protection of Privacy Act* (the Act).

A brief description for each transaction is provided. It is important to note that these refer to all duties and powers as set out in each of the sections of the Act. For example, in the case of sections 12-22.1, the head may refuse to disclose certain kinds of information but must not refuse to disclose other types of information. A user should therefore refer to the Act as necessary to complete the attached schedule.

Public bodies should delete any transactions that they do not wish to delegate.

Heads of police boards should be aware that, under s. 49(1.2), they may not delegate the authority to make a request to the Information and Privacy Commissioner under s. 49(1.1)(b).

Special Note regarding section 16

Under s. 16(2)(a), the Attorney General may give consent for disclosure of law enforcement information that falls under section 16(1). The Executive Council can give consent under s. 16(2)(b) for disclosure of other types of information that fall under section 16(1).

If you have Questions

Public bodies may call the Privacy and Access Helpline at 250 356-1851 or send an email to CPIAadmin@gov.bc.ca if they have any questions about this schedule.

Delegation of duties, powers and functions of the head of the public body under the *Freedom of Information and Protection of Privacy Act* – Broader Public Sector

A. DELEGATION BY THE HEAD OF THE PUBLIC BODY

Full name of public body

BC Oil and Gas Commission

Pursuant to section 66 of the *Freedom of Information and Protection of Privacy Act* (the Act), I hereby delegate my powers, duties and functions as head of the public body to the persons who hold the positions, and to the extent, set out in the attached Schedule, subject to the following conditions:

(a) that the persons to whom my powers, duties or functions are delegated are bound in the exercise of those powers, duties or functions by the jurisdictional, legislative and administrative limitations to which I am subject;

(b) that the powers, duties or functions delegated to any person may also be exercised by another person who holds the person's position in an acting capacity to which he or she has been duly appointed;

(c) that, notwithstanding the delegation of my powers, duties or functions, I may exercise at any time any of the powers, duties or functions delegated.

This delegation is effective on and from the date shown below and shall remain in effect until revoked.

This delegation may be revoked or amended from time to time.

Commissioner, CEO		June 15, 2022
Name and position title of the head of the public body	Signature	Date

B. SCHEDULE

This Schedule sets out the lowest level positions of individuals to whom powers, duties and functions of the head of a public body which is not a ministry are delegated.

This does not in any way limit the authority of individuals in positions directly above the listed positions from exercising any of the delegated powers, duties or functions in their areas of responsibility.

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
INFORMATION RIGHTS		
Duty to assist applicants Duty to assist applicants and create a record from a machine readable record	6	Specialist, FOIPP
Time limits for responding Must respond no later than 30 business days, with limited exceptions	7	Specialist, FOIPP
Contents of response Must tell applicant of entitlement to access to records. If access refused, tell applicant the reasons, subject to s. 8(2), and of the right to request a review	8	Specialist, FOIPP
How access will be given Must provide copies or allow examination of original records	9	Specialist, FOIPP
Extending the time limit for responding Must tell applicant of reason for extension, when a response can be expected and right to complain	10	Specialist, FOIPP
Transferring a request May transfer a request and, if necessary, a record within 20 days	11	Specialist, FOIPP
EXCEPTIONS		
Cabinet confidences Must refuse to disclose information revealing the substance of deliberations of the Executive Council or any of its committees	12(1)	Specialist, FOIPP

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
Local public body confidences May refuse to disclose draft resolutions, bylaws or other legal instruments or substance of deliberations of meetings of elected officials, governing body or a committee of governing body	12(3)	Specialist, FOIPP
Policy advice or recommendations May refuse to disclose advice or recommendations developed by or for a public body or a minister	13	Specialist, FOIPP
Solicitor client privilege May refuse to disclose information subject to solicitor client privilege	14	Specialist, FOIPP
Disclosure harmful to law enforcement May refuse to disclose information which could reasonably be expected to harm law enforcement	15	Specialist, FOIPP
Disclosure harmful to intergovernmental relations or negotiations May refuse to disclose information that could harm relations between the government of B.C. and other governments, including aboriginal governments	16	Specialist, FOIPP
Disclosure harmful to financial or economic interests of a public body May refuse to disclose information harmful to financial or economic interests of a public body or the government of B.C.	17	Specialist, FOIPP
Disclosure harmful to the conservation of heritage sites, etc. May refuse to disclose information that could damage or interfere with the conservation of fossil sites, heritage sites or endangered species	18	Specialist, FOIPP
Disclosure harmful to individual or public safety May refuse to disclose information which could threaten anyone else's safety or mental or physical health or interfere with public safety, or could cause applicant immediate and grave harm	19	Specialist, FOIPP

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
Information that will be published or released within 60 days May refuse to disclose information that will be published or released to the public within 60 days of receipt of the applicant's request, or that must be published or released to the public under an enactment	20	Specialist, FOIPP
Disclosure harmful to business interests of a third party Must refuse to disclose trade secrets, commercial, financial, labour relations or scientific information of or about a third party, that was supplied in confidence, **and** disclosure of which could cause harm to the third party	21	Specialist, FOIPP
Disclosure harmful to personal privacy Must refuse to disclose information that would be an unreasonable invasion of a third party's personal privacy	22	Specialist, FOIPP
Disclosure of information relating to abortion services Must refuse to disclose information that relates to the provision of abortion services	22.1(2)	Specialist, FOIPP
NOTICE TO THIRD PARTIES		
Notice to third party and applicant Public body **must** give third party a written notice when it intends to give access to a record containing information that it has reason to believe might be excepted from disclosure under s. 21 or 22 and **may** give third party notice when it intends to refuse access to information pursuant to s. 21 or s. 22	23	Specialist, FOIPP
Time limit and notice of decision Must decide within 30 days after notice is given under s. 23 to give access to all or part of record, provide applicant and third party with written notice of decision and tell third party of right to request a review	24	Specialist, FOIPP

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
PUBLIC INTEREST PARAMOUNT		
Information must be disclosed if in the public interest Must disclose information about a risk of significant harm to environment or to health or safety of public or group of people or disclosure of which is clearly in public interest	25	Commissioner, CEO
PROTECTION OF PRIVACY		
Right to request correction of personal information Must correct or annotate applicant's personal information on request	29	Specialist, FOIPP
Obligation to report foreign demand for disclosure Must notify the minister responsible for this Act if a foreign request for disclosure is received or unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure	30.2(2)	Commissioner, CEO
Notification of unauthorized disclosure Receive notification of unauthorized disclosure of personal information	30.5(2)	Specialist, FOIPP
Disclosure inside or outside Canada in compelling circumstances Determine that compelling circumstances exist affecting anyone's personal health or safety	33.1(1)(m)	Specialist, FOIPP
Disclosure inside or outside Canada for research or statistical purposes May approve conditions related to security and confidentiality, removal or destruction of individual identifiers and prohibition of subsequent use or disclosure of personal information	35(1)(c)	Specialist, FOIPP

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
Power to authorize a public body to disregard requests May ask commissioner for authorization to disregard requests that are frivolous or vexatious or would unreasonably interfere with operations of the public body due to their repetitious or systemic nature	43	Executive Vice President
Powers of commissioner in conducting investigations, audits or inquiries May require commissioner to examine original record at its site	44(4)	Executive Vice President
REVIEWS & COMPLAINTS		
Burden of Proof Must prove that an applicant has no right of access to a record in full or in part	57(1)	Specialist, FOIPP
Duty to comply with orders Must comply with order of commissioner under s. 54.1 or s. 58	59(1) & 59(1.1)	Specialist, FOIPP
GENERAL PROVISIONS		
Respecting use of Personal Information Must conduct a privacy impact assessment in accordance with directions of Minister responsible for this Act	69(5.3)	Specialist, FOIPP
Must submit a privacy impact assessment for any proposed enactment, system, project, program or activity to Minister responsible for this Act	69(5.4)	Specialist, FOIPP
Must notify commissioner of data-linking initiative or common or integrated program or activity	69(5.5)	Specialist, FOIPP
Must make available to public a directory listing its personal information banks	69(6)	Specialist, FOIPP
Policy manuals available without request Must make available policy manuals, instructions, guidelines, or substantive rules or policy statements adopted by public body	70	Specialist, FOIPP

TRANSACTION	SECTION	NAME OF POSITION & IF APPLICABLE, NAME OF PUBLIC BODY
Records available without request Must establish categories of records available to public without request for access under the Act	71	Specialist, FOIPP
Recovery of personal information May issue written notice demanding that a person or entity return information, securely destroy information or respond in writing to declare they are authorized by law to possess this information	73.1	Executive Vice President
Court order for return of personal information May ask Attorney General to petition superior court for order requiring return of personal information	73.2	Executive Vice President
Fees May require payment of fee	75(1)	Specialist, FOIPP
Must provide written fee estimate and may set amount of deposit required	75(4)	Specialist, FOIPP
May excuse all or part of fee	75(5)	Executive Vice President
Must respond in writing to the applicant's fee waiver request within 20 days	75(5.1)	Specialist, FOIPP

Summary of Responsibilities as FOIPPA Delegated Head

May 2023

Delegation under FOIPPA – Key Points

Source: Section 66 - Delegation by the Head of a Public Body - Province of British Columbia (gov.bc.ca)

Summary

The head of a provincial public body has full power to delegate any of the head's duties, powers or functions conferred under the Act (except the power to delegate) to another person. Normally, the head delegates to officers or employees of the public body (in the case of provincial government ministries, to the Deputy Minister). The delegation must be in writing and contain any conditions or restrictions the head of the public body considers appropriate.

The head of a local public body does not have authority to delegate any of the powers or function of the head. However, a local public body may accomplish the same administrative purpose by authorizing (through bylaw or other policy instrument) a person other that the head to perform any duties or functions of the head (see manual section 77(b)).

Policy

1. Only the head of a provincial public body has the power to delegate under the Act. An officer, employee or member to whom authority has been delegated does not have the power to re-delegate this authority.
2. The head of a provincial public body must make delegations in writing with any conditions or restrictions set out in the written delegation instrument.

Procedure

1. Provincial government ministries must create, file and maintain a valid delegation matrix clearly indicating the lowest level officer or employee of the ministry authorized to approve and accept transactions and sign formal documents.

Note: Provincial government is still in the process of updating templates to reflect the latest amendments to FOIPPA. An updated online version of the Delegation Instrument template for public bodies that includes new section 18.1 (Disclosure harmful to the interest of an Indigenous people), is still pending. Once available online, the BCER should complete and sign-off a new matrix.

Summary of Executive VP Responsibilities

TRANSACTION	DESCRIPTION	SECTION	RESPONSIBLE POSITION	ACTION
Freedom of Information (FOI) Requests				
Power to authorize a public body to disregard requests	Public body may ask OIPC commissioner for authorization to disregard requests that are frivolous or vexatious or would unreasonably interfere with operations of the public body due to their repetitious or systemic nature.	S. 43	Executive VP	The FOI team, with assistance from Legal, would draft a **letter of request for the EVP's signature** that provides: (1) evidence that the BCER has exercised considerable restraint and made every effort to assist the applicant; and (2) an explanation/evidence of how the request meets the specific criteria for s. 43.
Power to excuse FOI processing Fees	Public body may excuse all or part of a fee related to an FOI request.	S. 75(5)	Executive VP	The BCER's FOI team rarely issues fee estimates for requests – rather, we work with an applicant to narrow their request, or identify the records they're really interested in. Current process related to fee issuance is to **advise the ED, IST and EVP of a request where a fee estimate is recommended – fee estimate is not issued without approval.** If a fee has been issued and the applicant requests a fee waiver, only the EVP can grant one on behalf of the BCER.
OIPC Investigation of Complaint (FOI)				
Powers of commissioner in conducting investigations, audits or inquiries	Public body may require commissioner to examine original record at its site.	S. 44(4)	Executive VP	This would only occur if the BCER was asked to produce a record for review (in response to an OIPC complaint) and it was not practicable to make a copy of the record. We would only come to this conclusion after careful analysis and consideration. The request for onsite

				examination would likely consist of a **letter drafted by the FOI team and Legal** *(FOI team would confirm criteria, preferred method of communication, information required by the OIPC, etc. to support this).*
Protection of Privacy				
Recovery of personal information	Public body may issue written notice demanding that a person or entity return information, securely destroy information or respond in writing to declare they are authorized by law to possess this information	S. 73.1	Executive VP	Relates to a personal information incident, breach and/or theft (e.g., detected by BCER employees, contracted service provider, IT/security monitoring, etc.). The FOI team, with assistance from Legal, would draft a **letter of request for the EVP's signature.**
Court order for return of personal information	Public body may ask Attorney General to petition superior court for order requiring return of personal information	S. 73.2	Executive VP	**Actioned if written notice approach is not effective. Any activities related to a court order would be managed through Legal with input from relevant staff**, as required. Executive representation may include both EVP Delegated head and Chief Legal Counsel.

Summary of Commissioner & CEO Responsibilities

Note: This summary includes an anticipated action/response of the BCER. The information has not been reviewed by BCER's Legal Services.

TRANSACTION	DESCRIPTION	SECTION	RESPONSIBLE POSITION	ACTION
Public Interest Paramount				
Information must be disclosed if in the public interest	Public body must disclose information about a risk of significant harm to environment or to health or safety of public or group of people or disclosure of which is clearly in public interest.	S. 25	Commissioner & CEO	*Anticipated that Legal (under direction of Chief Legal Counsel) in collaboration with Leadership/Executive would lead an assessment of applicability based on legislation/ government's public interest disclosure policy to determine whether a*

				mandatory section 25 disclosure was necessary, and the steps involved.
Protection of Privacy				
Obligation to report foreign demand for disclosure	Public body must notify the minister responsible for this Act if a foreign request for disclosure is received or unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure.	S. 30.2(2)	Commissioner & CEO	Government's FOIPPA Manual states that s.30.2(2) applies to public bodies and their employees, and contracted service providers. Notice to the minister about a foreign demand for disclosure, as known or suspected, includes the following information: - the nature of the foreign demand for disclosure, - who made the foreign demand for disclosure, - when the foreign demand for disclosure was received, and - what information was sought by or disclosed in response to the foreign demand for disclosure. In addition, the notice should inform the minister of how the public body, service provider or employee plans to respond to the request. *Anticipated that this requirement would be lead/overseen by Legal, under the direction of Chief Legal Counsel.*

WHAT IS FOI?

The Freedom of Information and Protection of Privacy Act (FOIPPA) enables the public to request and obtain copies of records held by government public bodies, when those records are not routinely available. These requests are known as "FOI Requests".

Who does FOIPPA apply to?

FOIPPA applies to **public bodies**, including all BC provincial government ministries, agencies, boards, commissions, and provincial Crown corporations. It also applies to local public bodies such as municipalities, regional districts, universities, hospitals, school boards and self-governing professional bodies (such as the College of Physicians and Surgeons). FOIPPA does not apply to private sector organizations in BC.

What are a public body's main obligations under FOI?

Under FOIPPA, public bodies:

- Have a legislated 30-business day time limit to respond to FOI requests, with specific exceptions which allow the ability to grant extensions of time in appropriate circumstances.
- Must consider all responsive records available to an applicant, and make every reasonable effort to assist.
- Should complete a line-by-line review of records identified as "responsive" to a request to determine whether any information contained within them requires protection from disclosure.

What oversight body ensures that FOI is done appropriately throughout government?

The Office of the Information and Privacy Commissioner (OIPC) provides independent oversight and enforcement of BC's access and privacy laws. The OIPC is responsible for monitoring how FOIPPA is administered, and is authorized to conduct investigations and audits to ensure compliance with any provision of FOIPPA. Applicants have the right to request formal review of a decision, act or failure to act with respect to a public body's administration of a FOI request under FOIPPA.

What is considered a "record" under FOIPPA?

A record is any information recorded or stored by any means, whether in physical (hardcopy) or electronic format. This includes emails, notebooks, correspondence, photographs, phone records and even information on post-it notes. If it was created in the course of your daily work, it is considered a record.

Are all requested records released under FOI?

No. Records are not automatically released to the public. There are exceptions to the public's information rights under FOIPPA. For example, an applicant will not get access to Cabinet confidences, someone else's personal information, or information that could harm another individual's business interests. An applicant will also not get access to records that could harm law enforcement, or the economic or financial interests of a public body, other individuals or the public. *See "FOIPPA Exceptions to Disclosure" for details.*

Are all requests for information handled formally?

No. Some requests for information can be satisfied informally through routine channels. Through our corporate website, the Commission makes select records information available to the public. Over time, additional information will be proactively released as the Commission works to identify information suitable for disclosure as part of its *Transparency Strategy*.

A formal FOI request is necessary when there may be sensitive or confidential information contained within a record. For example, information that:

- Was created by or relates to another government public body or its employees
- Was provided by or is about a third party (e.g. a company's financial or proprietary business information)
- Relates to government negotiation or consultative processes
- Includes personal information about an individual (e.g. landowner information, information relating to employees, etc.)

The Commission's FOI staff, in collaboration with program subject matter experts and management, identifies whether information is unsuitable for release.

What should I do if I receive a written request for information?

If a program area receives a request for a record(s) that is identified as routinely releasable (no harmful or sensitive/confidential information exists within the record), staff may provide the record to the applicant.

If the requested record(s) contains or may contain sensitive/confidential information, is not a record that's made available to the public or you are unsure, please contact the Commission's FOI Specialist, Dana Keough or send an enquiry to the FOI team inbox at FOIintake@bcogc.ca

FOI IN THE COMMISSION

The Commission receives requests for information from multiple applicants (e.g., media, interest groups) for a wide variety of subjects. During 2015-2017, 170 requests were received and processed formally under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Where records are not available through routine venues, the Commission processes requests for information internally through a formal FOI process. Over time, the Commission is looking to make more information routinely available to the public which may help to reduce the number of formal requests received.

Commission FOI "At-A-Glance"

1. **Our external website features our corporate FOI inbox (FOIintake@bcogc.ca) and information for the general public on how to submit an FOI Request**

2. **We have staff dedicated to administering FOI requests and ensuring compliance:**

   - Dana Keough (FOIPP Specialist) and Kathryn Smerechinskiy (Director)
   - It requires a "small village" to do FOI effectively. We regularly consult with the Commission's communications and legal teams, plus many of you as the subject matter experts.

3. **We are establishing a new internal FOI process that includes:**

   - A single point of contact model within each program area, where one individual receives notification of new FOI requests, coordinates records searches within their team, and ensures responsive records are supplied to the Commission's internal FOI team in a timely manner.
   - An internal FOI review group comprised of VPs/Executive Directors and Program Leads to review and approve FOI packages prior to release.
   - Formal sign-off of FOI releases by the Delegated head (CFO & Executive VP, Corporate Services).

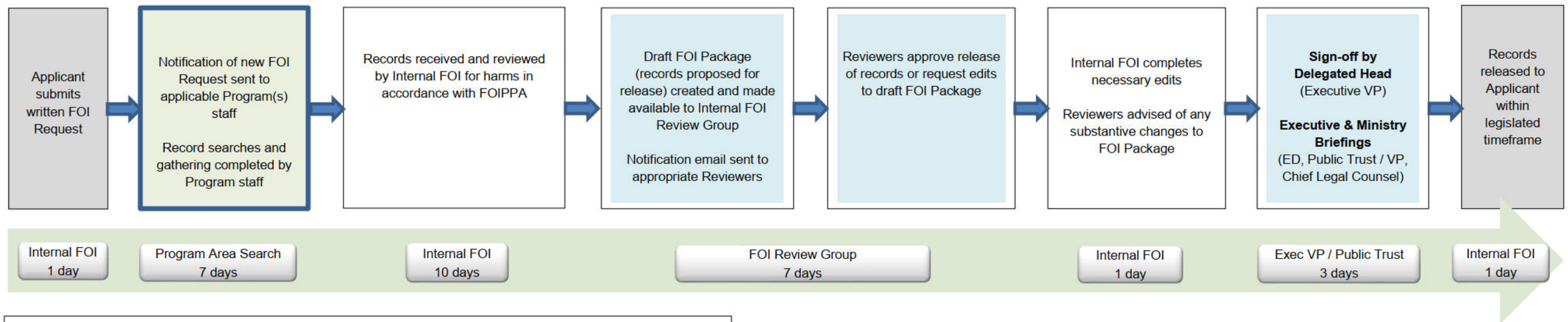
Our "Top 3" FOI Objectives

1. To build staff awareness about FOIPPA and their accountabilities under the Act.
2. To ensure adequate and thorough searches for records are conducted.
3. To promote openness and transparency while balancing the need to protect sensitive information.

What should I do if I receive a written request for information?

If a program area receives a request for a record that's identified as routinely releasable (no harmful or sensitive/confidential information exists within the record), staff may release the record to the applicant. If the requested record appears to contain sensitive/confidential information, is not a record that's typically made available to the public or you are just unsure, please contact the Commission's FOIPP Specialist or send an enquiry to the FOI team inbox at FOIintake@bcogc.ca

INTERNAL FOI PROCESS FLOWCHART



Flowchart reflects a typical 30 business day processing timeline:

Searches for Records
- 5-7 business days are typically allocated for records searches and gathering by Commission program areas.
- If record volumes are significant, a time extension may be taken or Fee Estimate issued to the Applicant.

FOIPPA Review by Internal FOI
- 2-10 days is typically allocated for a line-by-line review of responsive records by Internal FOI staff.
- Exceptions under FOIPPA are applied to information deemed harmful to release.
- Draft FOI Package is created for review by the internal FOI Review Group.

Review & Approval by Leadership Group Members
- 5-7 business days are typically allocated for review and approval of a FOI Package by FOI Review Group.
- This time period may be increased for large and complex files if additional time is available.
- Time may be reduced if the package is small or the legislated date for response is approaching.

Sign-Off by Delegated Head (Executive VP)
- Executive sign-off occurs when: (1) any required changes to a FOI Package have been completed; and (2) all required Review Group approvals have been received.

Release to Applicant
- Requested records are released to the Applicant after required briefings have been completed.

SECTIONS OF THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FOIPPA) / EXCEPTIONS TO DISCLOSURE

FOIPPA establishes an applicant's right to access records held by a public body. There are certain exceptions to accessing records. "Severing" or redactions are applied to records in accordance with these sections of FOIPPA. Four out of the 12 exceptions are mandatory (sections are identified in red below), with s.18.1 being the most recent exemption addressing Indigenous cultural protections. The other exceptions to disclosure can be applied at a public body's discretion. *An organization's approach to proactive release of records should align with FOIPPA's exceptions to disclosure, as well as any other applicable legislation related to the confidentiality of information.*

Section #	FOIPPA Section Title	High-Level Description of FOIPPA Disclosure Exemption
12	Cabinet Confidences	A provincial government public body must withhold information that would reveal Cabinet confidences (e.g. advice, recommendations, policy considerations or draft legislation/regulations submitted or prepared for submission).
13	Policy Advice, Recommendations or Draft Regulations	Covers information that would reveal advice or recommendations. This section is intended to allow for full and frank discussion of policy issues during deliberative processes.
14	Disclosure Harmful to Legal Advice	Covers communications between a public body and its legal counsel (protects solicitor client privilege).
15	Disclosure Harmful to Law Enforcement	Covers information that would harm a law enforcement matter.
16	Disclosure Harmful to Intergovernmental Relations or Negotiations	Covers matters which could harm the relations between BC's levels of government and governments from other provinces and jurisdictions (e.g. Government of Canada/Province of Canada, council of municipality, regional district board, aboriginal government, government of a foreign state, international organization of states).
17	Disclosure Harmful to Financial or Economic Harm	Covers information which, if released, would cause financial or economic harm to the public body or to the government.
18	Disclosure Harmful to Conservation of Heritage Sites	Covers information about heritage sites which would result in the exploitation or destruction of those sites.
18.1 (New)	Disclosure Harmful to Interests of an Indigenous People	Covers information that could reasonably be expected to harm the rights of an Indigenous people to maintain, control, protect or develop their cultural heritage, traditional knowledge, traditional cultural expressions, or manifestations of sciences, technologies or cultures.
19	Disclosure Harmful to Individual or Public Safety	Covers information that could result in harm to any person's mental, physical or emotional health or to public safety.
20	Information That Will Be Published or Released Within 60 Days	A public body may withhold information from an applicant if it is already for sale to the public, or if the public body plans to release or publish the information within 60 days.
21	Disclosure Harmful to Third Party Business Interests	Public bodies are often in possession of commercial or financial information of outside businesses and must withhold that information from an applicant if releasing it would cause harm to the business. A specific three-part test must be met in order to appropriately apply the section.
22	Disclosure Harmful to Personal Privacy	Personal information belongs to that individual. Except in very limited circumstances, public bodies must not release an individual's information to anyone else without their consent.

HARMS ASSESSMENT CHECKLIST

A guideline for identifying potentially harmful information in FOI release materials.

Use the following "checklist" as an aid for identifying information that could potentially be harmful if released:

1. Harm to other governments

- ☐ Do the records contain confidential negotiations with other governments?
- ☐ Do the records contain information that could harm our relationship with the Canadian government, another province, a municipality or regional district, an aboriginal government or international state or states?

2. Harm to the Commission

- ☐ Could release of information be harmful to our financial interests (e.g. information has monetary value)?
- ☐ Could release of information be harmful to our economic interests (e.g. could damage the economic policies/activities for which the Commission is responsible)?
- ☐ Do the records relate to administrative or personnel management plans that are not yet public?

3. Harm to 3rd party business interests

- ☐ Do the records contain information about a business's confidential negotiations with the Commission?
- ☐ Could release of information reveal the business's trade secrets?
- ☐ Was the information supplied in confidence?
- ☐ Could release of information harm the business's competitive position, result in the Commission no longer receiving the information, or result in undue financial losses or gains?

4. Legal advice

- ☐ Do the records contain legal advice?
- ☐ Was the information intended to be confidential?
- ☐ Was the record created for the purpose of seeking or giving legal advice?
- ☐ Do the records relate to a legal matter? If yes, is the matter still ongoing?
- ☐ Are the records being used in litigation?

5. Cabinet confidences

- ☐ Were the records submitted, or prepared for submission to Cabinet/Treasury Board?
- ☐ If yes, are they draft or a final submission?
- ☐ If yes, have the records gone to Cabinet, or are they pending?
- ☐ If they've gone to Cabinet, has the information been made public? Implemented?

6. Policy advice and recommendations

- ☐ Do the records contain information that is policy advice prepared for a public body or minister?
- ☐ Do the records consist of 'draft' materials / advice / recommended courses of action?

ISSUANCE: **Public and Corporate Relations Department**
Records Management Branch

APPROVED: **December 10, 2019**

1.0 GENERAL

1.1 Purpose

This Policy details the proactive disclosure of responses to General access to information requests (FOI Requests) in accordance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and the BC Oil and Gas Commission's (Commission) Proactive Disclosure Exemption Criteria.

1.2 Background

Transparency is one of the Commission's values and helps ensure openness and accessibility to information is incorporated in every aspect of the Commission's business. Supporting public access to information is the Commission's primary objective subject to applicable legislation and regulations.

1.3 Applicability

This Policy applies to all records, regardless of format, as they relate to general requests for information administered under FOIPPA. It does not replace, limit or extend an individual's right of access to information, or the Commission's obligations under FOIPPA. Rather, this Policy seeks to supplement the goals of FOIPPA and the values of the Commission, by encouraging the release of information and promoting transparency, while at the same time ensuring the protection of personal and other confidential information.

1.4 Authority

- *Freedom of Information and Protection of Privacy Act*
- *Copyright Act*

1.5 Definitions

- **Applicant** is the party making a request for access to records under FOIPPA. Examples of Applicant types include media, political party, researcher, industry and individual.
- **Contact information** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.
- **Confidential records** contain information requiring protection against unauthorized access or disclosure. Records are classified as confidential based on a variety of requirements, including but not limited to policy or legislation. For example, FOIPPA identifies exceptions to the disclosure of requested information. Examples of Commission confidential records include well data, where confidentiality periods apply as defined in the drilling and production regulations, and First Nation consultations and draft agreements.
- **Copyright** is the right to reproduce a work or any substantial part of a work. Records may be protected by copyright under the federal *Copyright Act*, pursuant to which unauthorized reproduction of works is forbidden. Permission of the copyright owner must be obtained prior to reproduction, dissemination or sale of the records.

- **FOIPPA** means the B.C. *Freedom of Information and Protection of Privacy Act*.
- **FOI Request** means an access request made under Part 2 of FOIPPA for records held by the Commission.
- **General FOI Request** means a request for records of a non-personal nature that potentially could be released, in whole or in part, to anyone.
- **Personal FOI Request** means a request for records containing personal information about an individual. The request may be made by the individual themselves, or an authorized representative acting on their behalf.
- **Personal Information** means recorded information about an identifiable individual other than contact Information.
- **Proactive Disclosure** means the public release of the Commission's responses to General FOI Requests.
- **Records** include books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.
- **Routine Release** means the public release of Commission information that is not in response to an FOI Request.
- **Transparency** means the Commission encourages openness in access to clear information and the Commission's decision-making processes, operations or actions.

2.0 POLICY

The following policy requirements apply to the proactive disclosure of responses to General FOI Requests:

2.1 Responses to General FOI Requests must be posted to the Commission's website, unless an exemption is approved.

2.2 Responses to General FOI Requests will include the response letter, response records and Applicant type (e.g. Media, Researcher, Business, etc.).

2.3 Responses to General FOI Requests will be available on the Commission's website for up to one year following the date of posting. Any Responses that result in a formal review by the Office of the Information and Privacy Commissioner (OIPC) may be removed from the website sooner than one year.

2.4 An exemption to posting a response to a General FOI Request may be approved where specific exemption criteria apply. Exemption criteria are set out in Section 3.0.

2.5 Responses to Personal FOI Requests must not be posted to the Commission's website.

2.6 Any personal information must be removed from General FOI Request response records in accordance with the FOIPPA before posting to the Commission's website. Applicant contact information within response letters is also removed.

2.7 A response to a General FOI Request must be posted to the Commission's website a minimum of:

- 72 hours after its release, if the response is sent or provided electronically to the Applicant; or
- Five business days after its release, if a hard copy is mailed to the Applicant.

3.0 PROACTIVE DISCLOSURE EXEMPTION CRITERIA

3.1 Responses to General FOI Requests will be considered for exemption from proactive disclosure and posting on the Commission's external website if they contain:

- Personal information or information that could lead to the identification of the Applicant or other persons.
- Information that may harm relations with a First Nation.
- Information that may harm relations with another government.
- Information that may harm a third party's business interests.
- Information that is not suitable for proactive disclosure based on a formal risk assessment that disclosure to the public may threaten the safety of a person or harm the security of any property or system.

3.2 Commission FOIPPA staff will recommend an exemption from proactive disclosure where one or more of the above criteria are met.

3.3 Commission Public and Corporate Relations staff (Executive Director or Director) must approve any recommended exemption.

4.0 RESPONSIBILITIES

4.1 Executive and management are responsible for:

- Leading the Commission in enhancing transparency and accountability through the increased release of Commission information.

4.2 Commission FOIPPA staff are responsible for:

- Preparing responses to General FOI Requests for posting in accordance with established processes and timelines.
- Recommending exemptions to the proactive disclosure of General FOI Requests in circumstances where established criteria is met.
- Ensuring responses to Personal FOI Requests are not published.
- Ensuring personal information is removed from General FOI Request responses before they are proactively disclosed.
- Updating the Commission's FOI Proactive Disclosure Policy as required.

4.3 Commission Public and Corporate Relations staff are responsible for:

- Approving exemptions to the proactive disclosure of General FOI Requests in circumstances where established criteria is met.
- Providing information to Commission FOIPPA staff on relevant Copyright matters.
- Advising the public of the Commission's FOI Proactive Disclosure Policy.

5.0 APPROVAL:

Commissioner, Chief Executive Officer	Executive Vice President, Chief Financial Officer	Executive Vice President, Chief Operating Officer
Executive Vice President, Chief Engineer	Executive Vice President, Legal and Regulatory Affairs	

Version Control:

Document Created	Dec-19	Executive Approval

ISSUANCE: **Corporate Services Division**
Finance & Administration Department

APPROVED: **August 10, 2018**

1.0 GENERAL

1.1 Purpose

The BC Oil and Gas Commission (Commission) views information as an important and strategic asset that must be appropriately managed throughout its lifecycle according to legislated requirements. This policy details the roles, responsibilities and principles for the effective and compliant management of Commission records.

1.2 Background

The Commission is subject to the statutory requirements of the *Information Management Act* (IMA) which requires the digitization of non-digital records (subject to specific exemptions) and the use of appropriate information management systems.

1.3 Applicability

This policy applies to all records, regardless of format, that are created or received by the Commission and its employees in the course of their duties. It also applies to contractors, consultants and agents of the Commission who have access, custody or control of Commission records.

1.4 Authority

- *Information Management Act*
- *Interpretation Act*
- *Electronic Transactions Act*
- *Oil and Gas Activities Act*

1.5 Definitions

- **Active records** are records referred to frequently for daily business operations, or that need to be retained and easily accessible on site (if records exist in physical format).
- **Administrative records** support common organizational functions such as the management of facilities, property, finance, personnel, and information systems. These records are managed (classified and scheduled) in accordance with the government Administrative Records Classification System (ARCS).
- **Confidential records** contain information requiring protection against unauthorized access or disclosure. Records are classified as confidential based on a variety of requirements, including, but not limited to, policy or legislation. For example, the *Freedom of Information and Protection of Privacy Act* (FOIPPA) identifies exceptions to the disclosure of requested information. Examples of Commission confidential records include well data, where confidentiality periods apply as defined in the drilling and production regulations, and First Nations

consultations and draft agreements.

- **Digital (electronic) records** consist of information that is entered, created, manipulated and/or stored on digital media or storage devices, and includes:
  - Records that are born digital;
  - Digitized records (converted from non-digital format);
  - Unstructured data (e.g. documents); and
  - Structured data maintained within electronic systems.
- **Electronic Document and Records Management System (EDRMS)** is an integrated software system capable of managing both electronic and physical records through their life cycle in accordance with ARCS, ORCS and other approved records schedules.
- **Inactive records** are no longer required for ongoing business. These are records that are ready for final disposition or, in other words, records for which the scheduled active and semi-active retention periods have lapsed.
- **Information management** is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Operational records** relate to those mandated functions which are unique to a government public body, for which it is responsible for performing according to statute, regulation or policy. These records are described in an Operational Records Classification System (ORCS).
- **Records** include any recorded information created or received, and retained in the day to day operations of business. This covers "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise" as defined in the *Interpretation Act*.
- **Recordkeeping system** within a government office refers to a shared ARCS and ORCS based filing system in which official (non-transitory) records are organized, retained and disposed of according to approved record retention schedules. A recordkeeping system may consist of physical files in a file room, electronic folders and records saved on a shared drive, or an Electronic Document and Records Management System (EDRMS).
- **Retention schedule** provides a timetable for maintaining an organization's records. It governs the life cycle of a file from creation, through active use to inactive storage (when appropriate) to final destruction or their transfer to the custody and control of the Provincial Archives. The approved retention schedules for government records are defined in ARCS and ORCS and are applied throughout a records life cycle.
- **Semi-active records** are used only occasionally and do not need to be maintained in the office space of the Commission. While they still have value, they can be stored in economical, offsite storage facilities.
- **Transitory records** are records of temporary usefulness that are not an integral part of an administrative or operational record series. Transitory records are not required to meet statutory obligations or to sustain administrative or operational

functions. As with all records, they can exist in any format or medium (paper or electronic). These records are not regularly filed with official Commission records within filing systems.

2.0 PRINCIPLES OF INFORMATION MANAGEMENT

The Commission must manage its digital (electronic) and physical (hardcopy) records in accordance with legislated requirements and government-wide policies and standards for recordkeeping.

2.1 Access to Records

Records are a corporate asset and resource, and need to be accessible and shared by staff where appropriate. Access to sensitive or confidential records will be restricted to individuals whose duties require such access, in adherence with applicable information security classifications.

2.2 Duty to Document

Employees must create and maintain complete and accurate records sufficient to document evidence of their business activities, transactions, policy or decisions.

2.3 Digital (Electronic) Records

Records created or received in digital (electronic) format shall be treated as the authoritative records source and remain in digital (electronic) format. As both the Commission and BC government move to a digital recordkeeping environment, printing and filing records in hardcopy should be avoided where feasible. Physical records may be digitized and stored electronically as the authoritative source, provided government's digital conversion standards are met. Destruction of any physical records after their digitization must be approved and documented by the Commission's records management staff.

2.4 Recordkeeping

Program areas are responsible for maintaining a shared office recordkeeping system for official active records. Records form corporate memory and must be incorporated into the shared recordkeeping system upon creation or as soon as practical. Government legislation requires the filing and retention of records in accordance with approved government records classification and retention schedules.

2.5 Records Disposition

When records reach their inactive stage they are ready for final disposition review. Records management staff will carry out the review and determine whether records require further retention or disposal. Commission records are not to be destroyed or disposed of without approval from the designated Corporate Records Officer.

2.6 Records Storage

When records become semi-active they will be moved into the applicable records storage facility (physical records) or managed within a secure records environment (electronic records) as determined by the Corporate Records Officer or prescribed in the Commission's records management procedures.

3.0 RESPONSIBILITIES

3.1 Executive and management are responsible for:

- Cultivating an organization-wide culture that values records and information management;
- Enforcing policy and procedures for the proper collection, creation, storage, access, retention and disposal of information; and
- Ensuring proper levels of protection are applied to confidential information under their custody and or control.

3.2 Each employee is responsible for:

- Managing their records in accordance with appropriate records retention schedules, policies, procedures and best practices;
- Understanding, identifying and routinely disposing of transitory information created or received; and
- Protecting records in their custody or under their control from unauthorized disclosure, inadvertent loss or destruction.

3.3 Commission records management staff are responsible for:

- Delivering an efficient and effective Records Management Program that offers succinct processes, solutions, and records management strategies;
- Providing Commission-wide records retention schedule(s), data plans, policies, procedures and guidelines related to collection, creation, storage, access, retention and disposal of records;
- Assessing organizational training and resource support needs, and developing appropriate plans and materials to address these;
- Assisting in defining records management business requirements and integrating information management planning into systems, plans and budgets and;
- The approval of and secure disposal of records.

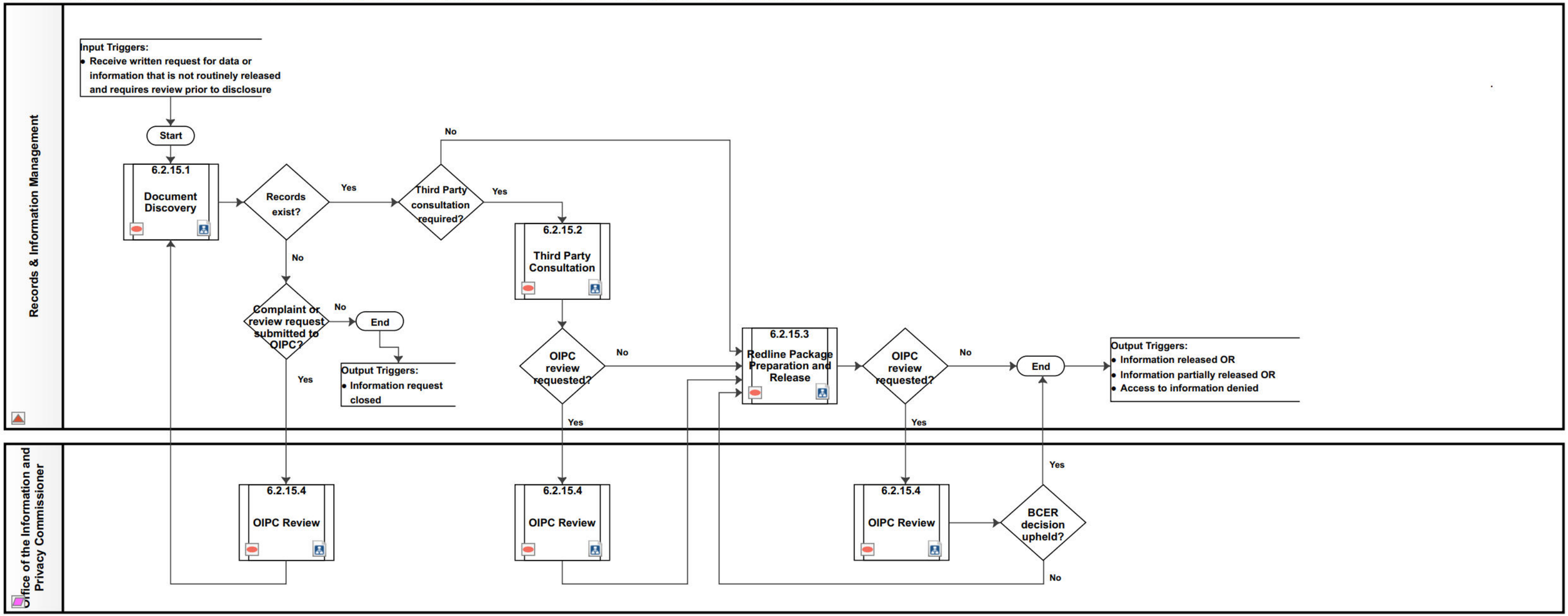
APPROVAL:

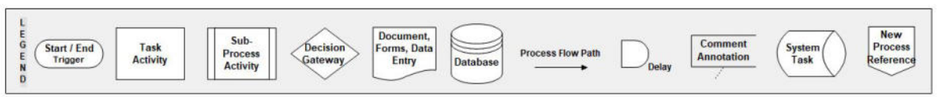
Commissioner, Chief Executive Officer	Executive Vice President, Chief Financial Officer	Executive Vice President, Chief Operating Officer
Executive Vice President, Chief Engineer	Executive Vice President, Chief Legal and Regulatory Officer	

Version Control:

Document Created	Aug-18	

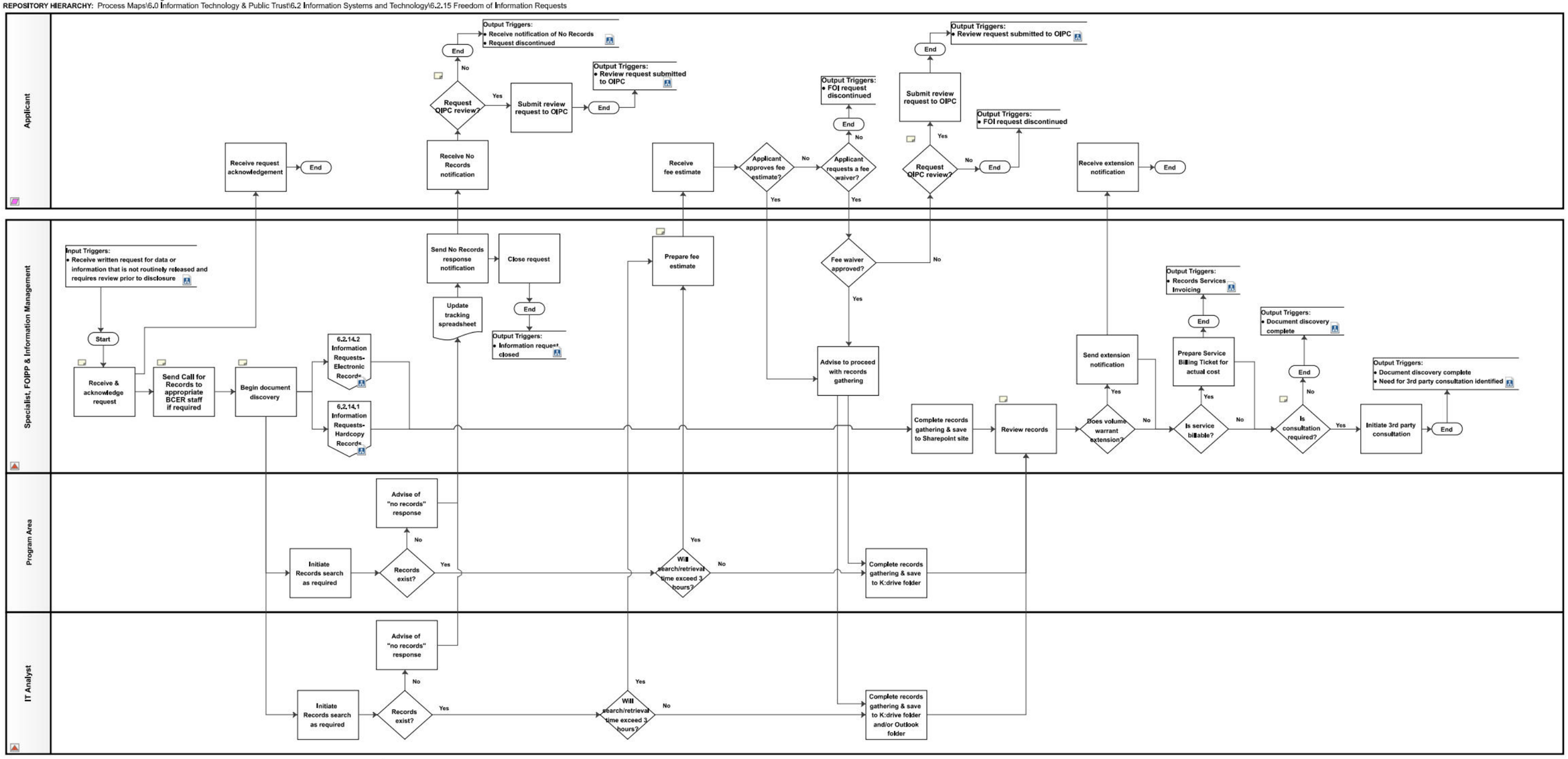
PROCESS NAME: **6.2.15 Freedom of Information Requests**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.15 Freedom of Information Requests





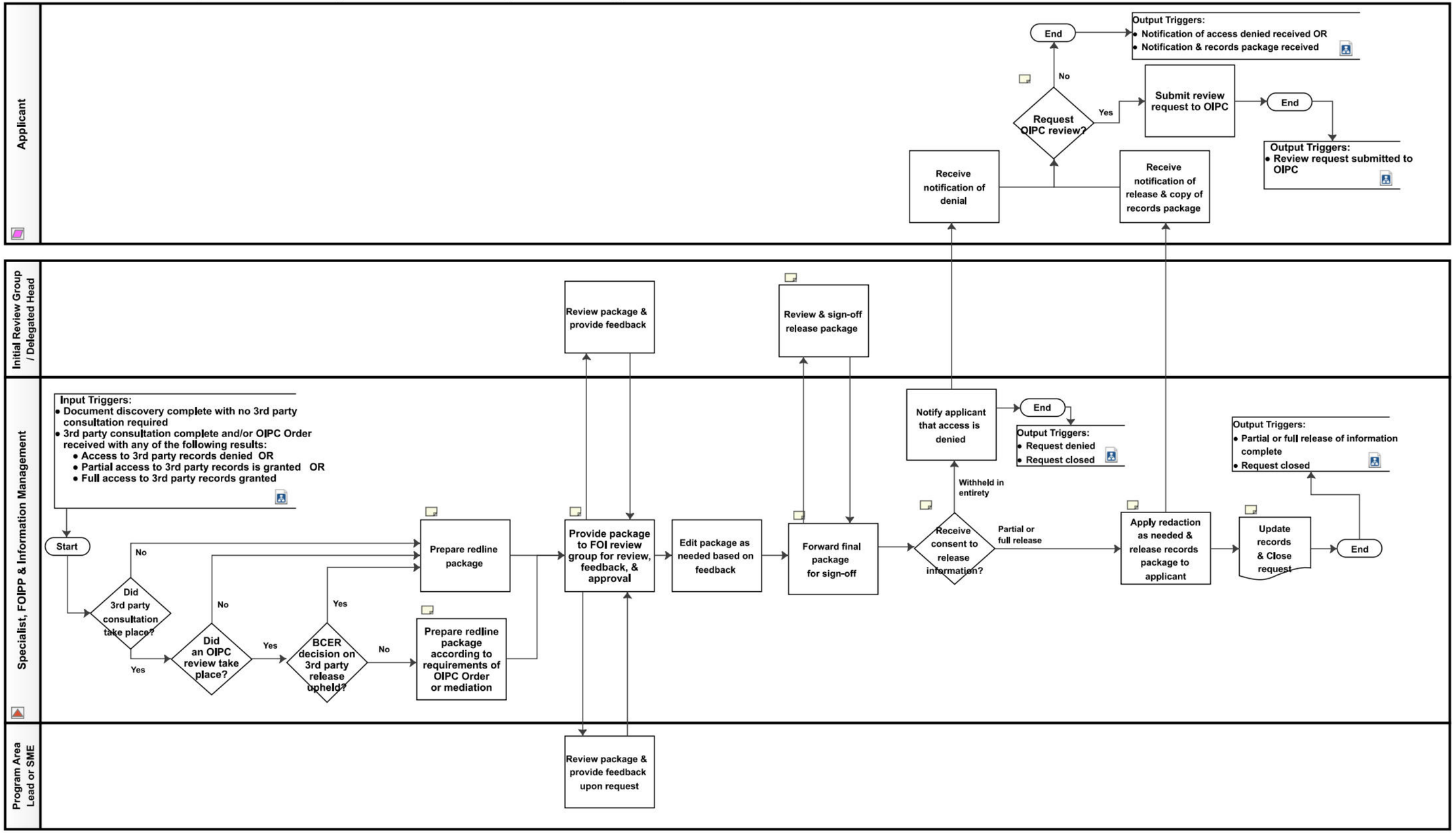
REVISED: 2023-09-18 15:37:48.0
DIAGRAM VERSION: 1.0.2

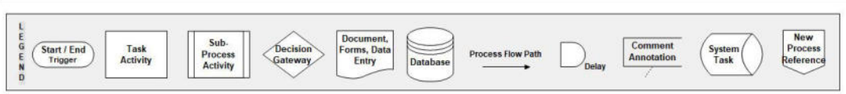
PROCESS NAME: **6.2.15.1 Document Discovery**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.15 Freedom of Information Requests



REVISED: 2023-09-18 15:47:10.0
DIAGRAM VERSION: 1.0.1

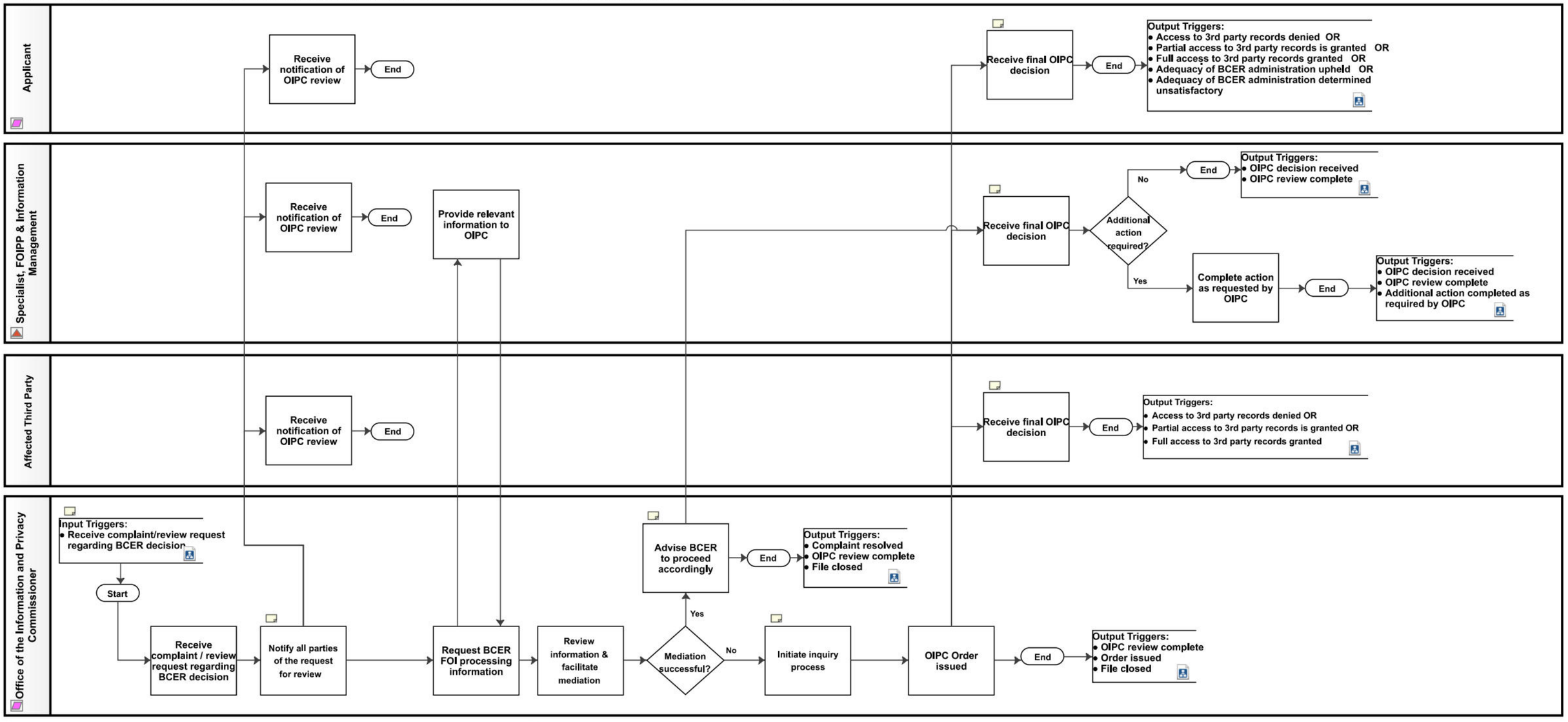
PROCESS NAME: **6.2.15.3 Redline Package Preparation**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.15 Freedom of Information Requests

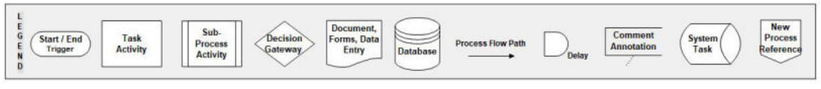




REVISED: 2023-09-18 15:59:29.0
DIAGRAM VERSION: 1.0.1

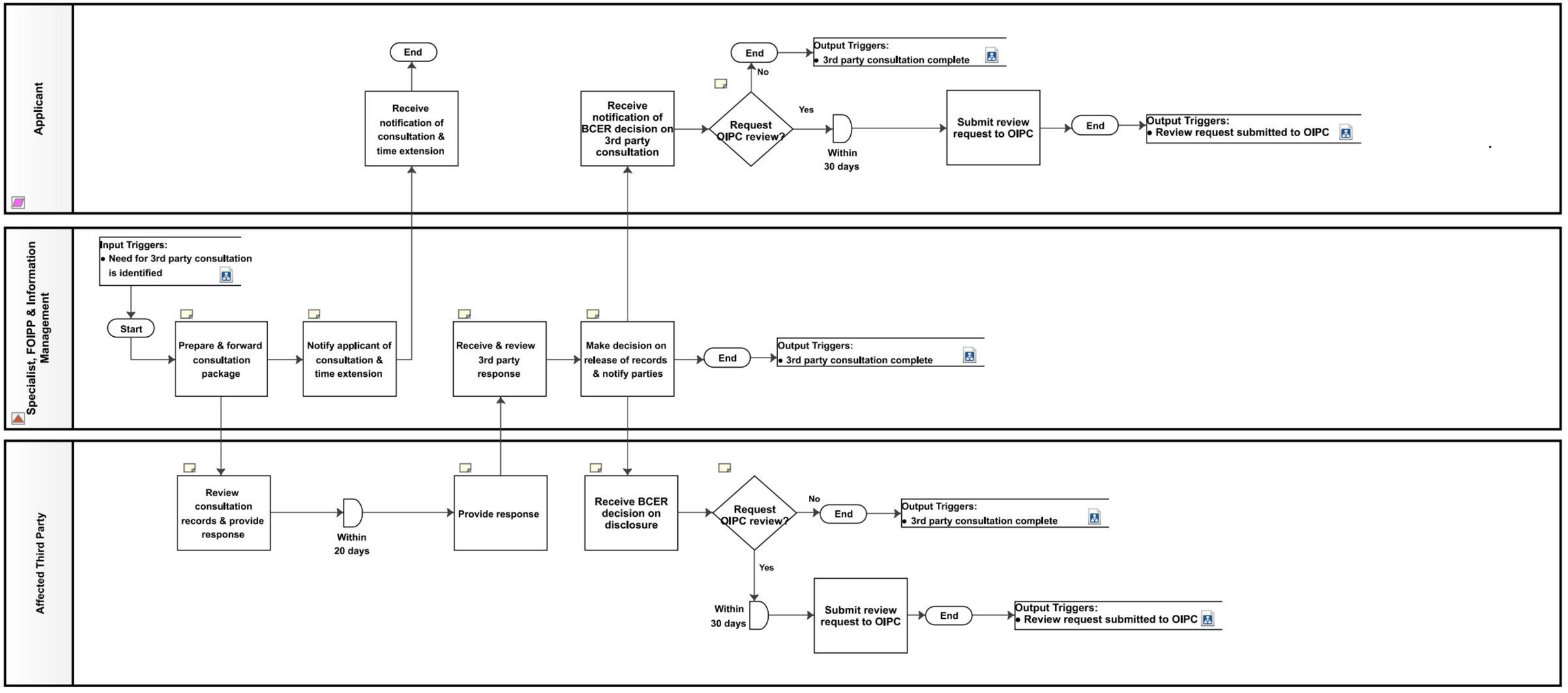
PROCESS NAME: **6.2.15.4 OIPC Review**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.15 Freedom of Information Requests

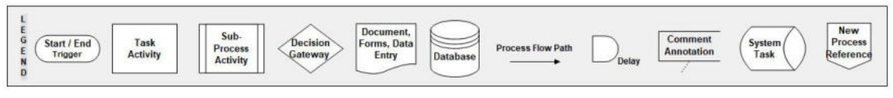




REVISED: 2023-09-18 16:06:16.0
DIAGRAM VERSION: 1.0.1

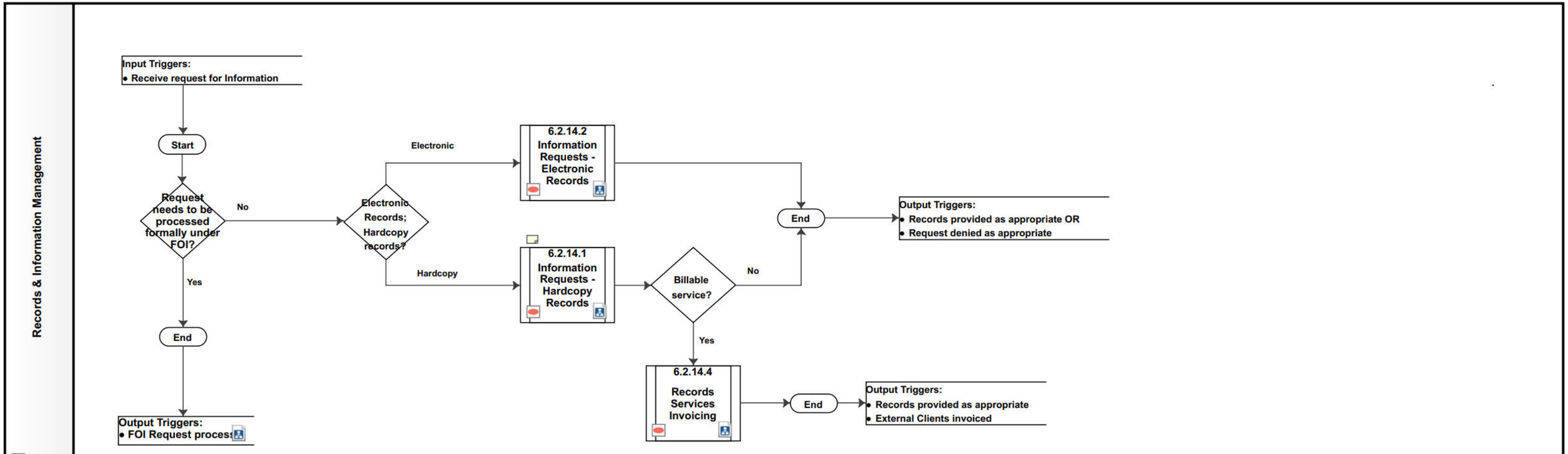
PROCESS NAME: **6.2.15.2 Third Party Consultation**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.15 Freedom of Information Requests

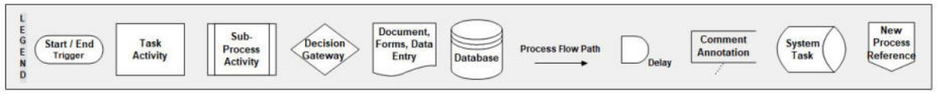




REVISED: 2023-09-18 15:53:21.0
DIAGRAM VERSION: 1.0.1

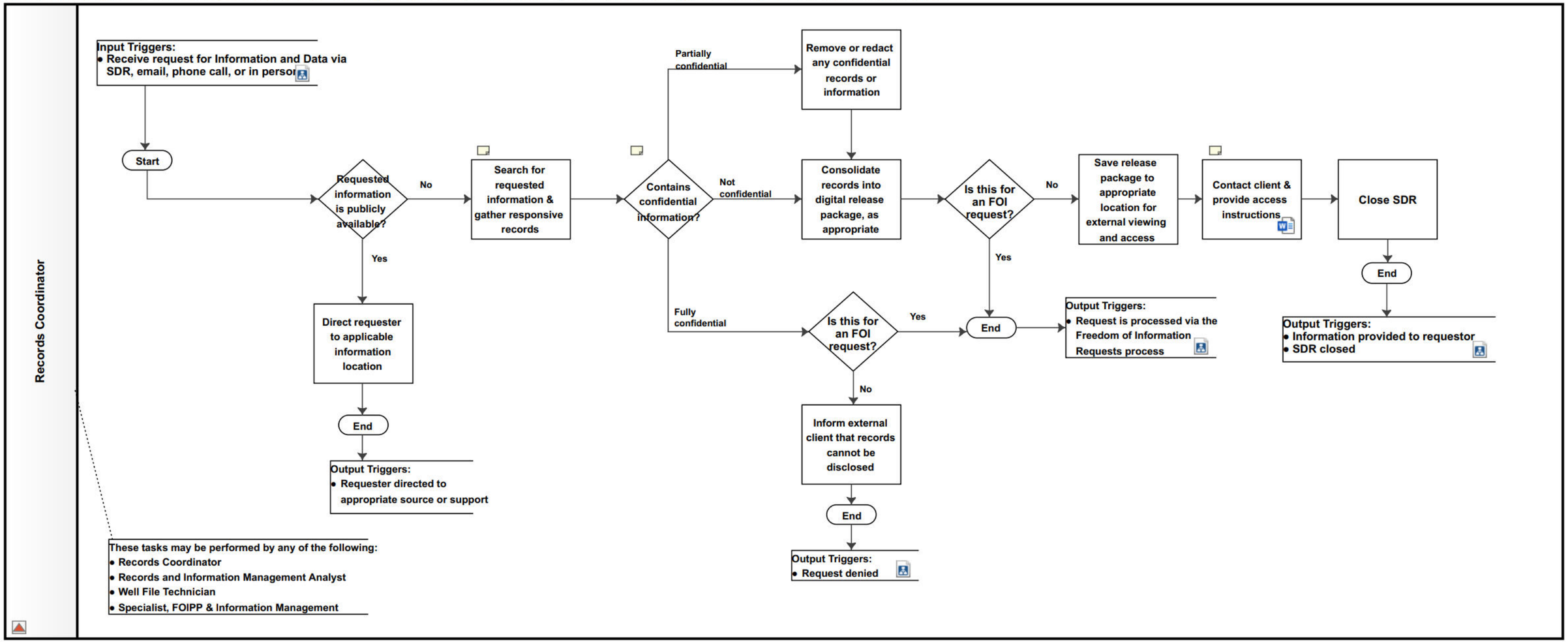
PROCESS NAME: **6.2.14 Routine Information Requests**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.14 Routine Information and Data Requests

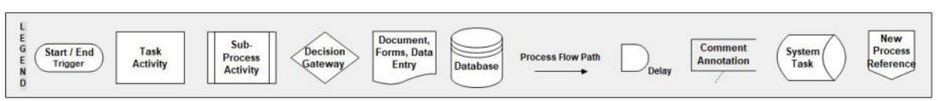




REVISED: 2023-09-18 15:17:39.0
DIAGRAM VERSION: 1.0.0

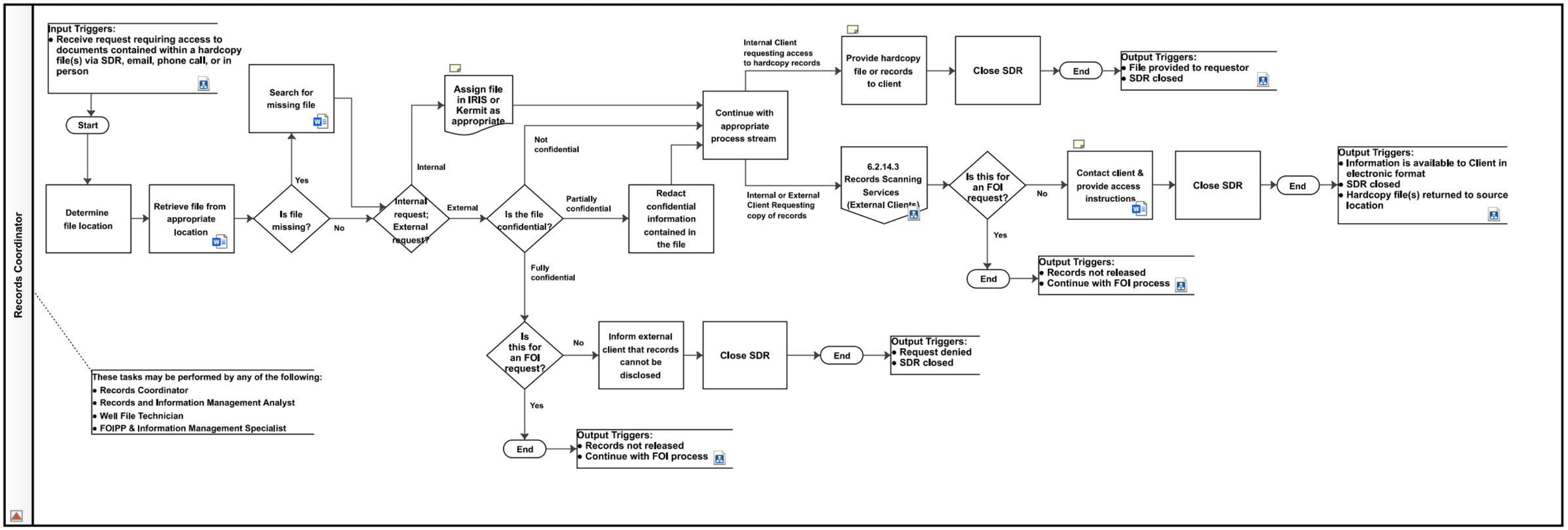
PROCESS NAME: **6.2.14.2 Information Requests - Electronic Records**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.14 Routine Information and Data Requests





REVISED: 2023-09-18 15:04:40.0
DIAGRAM VERSION: 1.0.0

PROCESS NAME: **6.2.14.1 Information Requests - Hardcopy Records**
PROCESS MANAGER: Executive Director, Information Systems & Technology
PROCESS OWNER: Vice President, Digital Transformation & Public Trust
REPOSITORY HIERARCHY: Process Maps\6.0 Information Technology & Public Trust\6.2 Information Systems and Technology\6.2.14 Routine Information and Data Requests



REVISED: 2023-09-18 15:11:15.0
DIAGRAM VERSION: 1.0.0