

Columbia Power Corporation

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/columbia-power-corporation/>

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.).

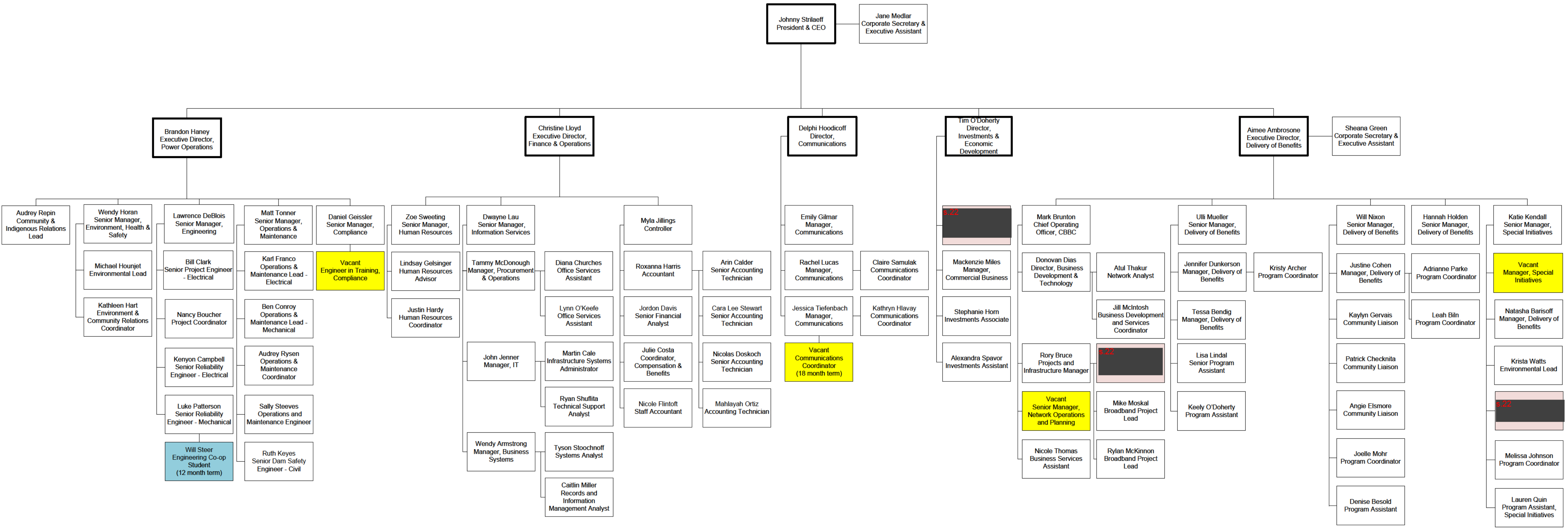
Summary

-

Rational

-

Columbia Basin Trust Organizational Chart



EMC

Vacant

On Leave

Temporary

MEMORANDUM

TO: Garry Merkel, Chair
FROM: Nancy Boucher
DATE: November 17, 2008
SUBJECT: Delegation of Authority

Purpose:

1. The purpose of this memorandum is to request delegation from the Chair of Columbia Basin Trust to the CEO/President with respect to Section 77 of the *Freedom of Information and Protection of Privacy Act (FOIPPA)*.

Discussion:

2. Columbia Basin Trust received a Freedom of Information Request with respect to the Head of the public body's calendar. Upon reviewing the request, it was noted that in Schedule 2 of the *Freedom of Information and Protection of Privacy Act*, the Head of Columbia Basin Trust is the Chair of the Board of Directors. Schedule 2 is a list of all of the organizations to which FOIPPA applies. The Schedule also specifies the position within the organization that is responsible for making decisions under the Act.
3. In some cases, Schedule 2 names the CEO (e.g. Columbia Power Corporation) as the Head of the Public Body and in other cases the Chair of the Board (e.g. BC Hydro) is named.
4. The Act provides for delegation authority from the position named in Schedule 2 to another position in the organization. Generally, where the Chair is named as the Head of the Public Body, authority has been delegated to other positions in the organization (for example, BC Hydro). Viewing Schedule 2 of the Act, and further investigation, it was found that wherein the Chair is the Head of the Public Body, the Chair has delegated his/her authorities down to the CEO/President.

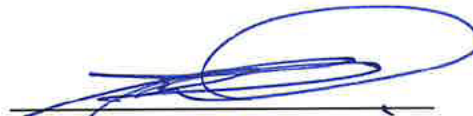
Recommendation:

5. In accordance with general practices under FOIPPA, it is recommended that you delegate all authorities under FOIPPA to the CEO/President. If you agree, the delegation instrument is attached for you to sign.

Recommended:


Neil Muth, CEO/President

Approved:


Garry Merkel, Chair

Delegation of authority under the
Freedom of Information and Protection of Privacy Act
and regulations thereunder

COLUMBIA BASIN TRUST

Pursuant to section 66 of the *Freedom of Information and Protection of Privacy Act* (the Act), I hereby delegate my powers, duties, and functions to the persons who hold the positions, and to the extent, set out in the Schedule, attached, 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.

Dated at Vancouver, BC this 21 day of November, 2008



GARRY MERKEL

Signature of Head of Public Body

SCHEDULE TO DELEGATION INSTRUMENT

This Schedule sets out the lowest level positions of individuals to whom powers, duties, and functions of the head 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 & NAME OF PUBLIC BODY
INFORMATION RIGHTS		
Duty to assist applicants All duties and powers set out in this section	6	CEO/President Columbia Basin Trust
Time limits for responding All duties and powers set out in this section	7	CEO/President Columbia Basin Trust
Contents of response All duties and powers set out in this section	8	CEO/President Columbia Basin Trust
How access will be given All duties and powers set out in this section	9	CEO/President Columbia Basin Trust
Extending the time limit for responding All duties and powers set out in this section	10	CEO/President Columbia Basin Trust
Transferring a request All duties and powers set out in this section	11	CEO/President Columbia Basin Trust
EXCEPTIONS		
Cabinet and local public body confidences Must refuse to disclose to applicant	12(1)	CEO/President Columbia Basin Trust
May refuse to disclose to applicant	12(3)	CEO/President Columbia Basin Trust
Policy advice or recommendations All duties and powers set out in this section	13	CEO/President Columbia Basin Trust
Legal Advice All duties and powers set out in this section	14	CEO/President Columbia Basin Trust
Disclosure harmful to law enforcement All duties and powers set out in this section	15	CEO/President Columbia Basin Trust
Disclosure harmful to intergovernmental relations or negotiations All duties and powers set out in this section	16	CEO/President Columbia Basin Trust
Disclosure harmful to the financial or economic interests of a public body All duties and powers set out in this section	17	CEO/President Columbia Basin Trust
Disclosure harmful to the conservation of heritage sites, etc. All duties and powers set out in this section	18	CEO/President Columbia Basin Trust
Disclosure harmful to individual or public safety All duties and powers set out in this section	19	CEO/President Columbia Basin Trust
Information that will be published or released within 60 days All duties and powers set out in this section	20	CEO/President Columbia Basin Trust
Disclosure harmful to business interests of a third party All duties and powers set out in this section	21	CEO/President Columbia Basin Trust

Disclosure harmful to personal privacy All duties and powers set out in this section	22	CEO/President Columbia Basin Trust
Disclosure of information relating to abortion services Must refuse to disclose information to applicant	22.1(2)	CEO/President Columbia Basin Trust
NOTICES TO THIRD PARTIES		
Notifying the third party All duties and powers set out in this section	23	CEO/President Columbia Basin Trust
Time limit and notice of decision All duties and powers set out in this section	24	CEO/President Columbia Basin Trust
PUBLIC INTEREST PARAMOUNT		
Information must be disclosed if in the public interest All duties and powers set out in this section	25	CEO/President Columbia Basin Trust
PROTECTION OF PRIVACY		
Right to request correction of personal information All duties and powers set out in this section	29	CEO/President Columbia Basin Trust
Obligation to report foreign demand for disclosure Notification of minister responsible for Act	30.2(2)	CEO/President Columbia Basin Trust
Notification of unauthorized disclosure Receive notifications of unauthorized disclosure	30.5	CEO/President Columbia Basin Trust
Disclosure inside or outside Canada Determination that compelling circumstances exist	33.1(1)(m)	CEO/President Columbia Basin Trust
Power to authorize a public body to disregard requests Ask the commissioner to disregard requests	43	CEO/President Columbia Basin Trust
Powers of commissioner in conducting investigations, audits or inquiries Require commissioner to view document at site	44(4)	CEO/President Columbia Basin Trust
REVIEWS & COMPLAINTS		
Duty to comply with orders Must comply with order of commissioner	59(1)	CEO/President Columbia Basin Trust
GENERAL PROVISIONS		
General information respecting the use of personal information Must correct errors/omissions in directory	69(4)	CEO/President Columbia Basin Trust
Must conduct privacy impact assessment	69(5)	CEO/President Columbia Basin Trust
Must prepare an information sharing agreement	69(5)	CEO/President Columbia Basin Trust
Must make directory available for inspection	69(6)	CEO/President Columbia Basin Trust
Policy manuals available without request All duties and powers set out in this section	70	CEO/President Columbia Basin Trust
Records available without request All duties and powers set out in this section	71	CEO/President Columbia Basin Trust
Fees	75(1)	CEO/President

Require payment of fee		Columbia Basin Trust
Excuse all or part of fee	75(5)	CEO/President Columbia Basin Trust
Must respond in writing within 20 days	75(5.1)	CEO/President Columbia Basin Trust

TO: Executive Management Committee

FROM: Dwayne Lau

DATE: January 26, 2022

SUBJECT: *Freedom of Information and Protection of Privacy Act (FOIPPA)*
Amendments - For Information

Purpose:

1. The purpose of this memo is to inform the committee of legislative amendments that were made to the Act, and the expected impacts on our business operations.

Summary:

2. The Act has been amended with key highlights included in this memo.
3. There are some operational impacts, though these are not considered significant.
4. The privacy department will be communicating changes to the organization departmentally, and organizationally as appropriate.

Background:

5. Amendments to the Act included in Bill 22 achieved Royal Assent on November 25th, 2021.
6. The majority of amendments came into force at the date of Royal Assent, with the exception of Section 25 which includes privacy management programs and breach notifications.
7. Section 25 is expected to come into force in the near future by regulation of the Lieutenant Governor in Council, which will clarify requirements and details.
8. The Privacy Department attended an information session on the amendments for agencies, boards and crown corporation on December 9, 2021.
9. A summary of key changes to the Act:

Section	Change	Operational Impacts
33.1 Disclosure outside of Canada	The change allows personal information to be stored outside Canada. Emphasis has been placed on a risk based approach to assessing privacy impacts.	<ul style="list-style-type: none">• The change allows the Trust to consider tools (i.e. cloud software) that would have previously been off limits

		<ul style="list-style-type: none"> Privacy Impact Assessments (PIA's) are already in place, regardless of data storage location. PIA's will be approached with greater rigor when data residency outside of Canada is identified Additionally, the privacy department will ensure IT completes a security assessment
Section 75 Fees	A public body may require an application fee of \$10	<ul style="list-style-type: none"> The practice of the Trust has been to not apply a fee to any FOI request We do not expect to change this practice unless the volume of FOI's increased significantly, or a specific request/applicant warrants a fee consideration
Section 65 Penalties	Penalties for 'willfully commits an offence under the Act' have increased for a corporation to \$500,000	<ul style="list-style-type: none"> No impact The Trust will continue to comply with the Act
Section 18.1	Public body must refuse to disclose information that could reasonably harm the rights of Indigenous peoples	<ul style="list-style-type: none"> This exception, along with existing exceptions will be considered as part of the FOI process by the Privacy department. The head of the public body (delegated to CEO of the Trust) makes final decision on information disclosed or excepted as part of FOI release
Section 25 Privacy management programs and breach notifications	<ul style="list-style-type: none"> Public bodies must develop a privacy management program. Public bodies must notify individuals, and the commissioner, if a breach could reasonably be 	<ul style="list-style-type: none"> We believe that the current privacy related policies, procedures, manuals, and practices of the Trust combine to form a management program. The privacy department will look at a future project to formalize this work into a documented program.

	expected to result in significant harm	<ul style="list-style-type: none">• We will assess the regulation regarding breaches for impacts, when it is provided.
--	--	--

Discussion:

10. The Trust currently has good privacy practices and strong general knowledge amongst staff regarding our requirements under the Act.
11. Changes in staffing in key public service areas of the organization requires continuous training to ensure our practices and knowledge remain strong.
12. The Privacy Department will request to attend department meetings over the next several months to communicate changes to the Act and associated impacts.
13. An intranet news post will be published highlighting changes to the Act.
14. The content for the yearly all staff FOIPPA training session, next scheduled for May, will be modified to reflect changes to the Act.

RECORDS & INFORMATION MANAGEMENT ANALYST

SUMMARY

The Records & Information Management Analyst is responsible for working to examine, maintain, automate, and improve records management processes while ensuring the organization's electronic document and records management programs are compliant under the information management program. This position reports to the Manager, Business Systems.

KEY ACCOUNTABILITIES

1. Provides records management program support.

- Coordinates offsite storage and retrieval for compliance with retention periods, agreement conditions and budgets.
- Purges, processes, and transfers records in all media for semi-active and inactive storage or destruction, according to approved records retention schedule.
- Supports and delivers internal Records Management Program compliance audits.
- Conducts analysis, maintains and updates the current functional classification structure, retention schedule and records disposition schedule and manages changes.
- Liaises with internal and external records and information management subject matter experts in determining departmental records projects.
- Delivers yearly compliance training on records and information management topics.
- Acts as the designated Records Officer contact when liaising with the BC Government.
- Creates reference guides, procedures and learning materials, as needed.

2. Provides electronic document and records management system support.

- Supports and maintains SharePoint sites containing corporate records.
- Assists with systems configuration design, development and customization of sites, libraries, lists, views, and workflows using SharePoint Online and Microsoft 365 Power Platform.
- Ensures compliance within the information management framework, including privacy, security, risk and records under the legislative areas of the Freedom of Information (FOI) and Personal Protection, Information Management programs.
- Analyzes processes to identify potential areas to improve automation of records management and policy administration using SharePoint and Microsoft's records management functions.
- Examines records management processes and identifies potential areas where existing business processes require change, or where new ones need to be developed.
- Analyzes existing information workflows, data storage and control procedures to identify opportunities for increased efficiencies and improvements in the sharing of information.
- Supports automated solutions with business intelligence based on best practices for SharePoint integration with other Microsoft products.
- Acts as a subject matter expert on the organization's information processes including storage, archival, retrieval and sharing of information.
- Supports and assists in analysis of eDiscovery processes for FOI requests or other related business analytic needs.
- Monitors and analyzes system performance and effectiveness and provides reports.
- Maintains systems administration documentation for use, as needed.
- Liaises with the Systems Analyst role to provide business analysis and backup support as necessary.

3. Performs other related duties as required.

QUALIFICATIONS

Training and Experience

- A minimum of a diploma in Business Administration, Library Sciences, OR an equivalent combination of education, training and experience.
- A minimum of two (2) years of experience working at an intermediate level of information management.
- Training or experience working with ARCS/ORCS or other classification systems and the development of policies, procedures and standards.
- Experience with SharePoint online and/or as a Microsoft Teams super user is an asset.
- Having accreditation as a Certified Records Manager (CRM), Information Governance Professional (IGP), Certified Information Professional (CIP), or other Rim certification is an asset.
- A high level of understanding of modern document management systems would be considered an asset.

Knowledge, Skills, and Abilities

- Strong knowledge of records management best practices and industry standards.
- Working knowledge of SharePoint online administration and management.
- Up to date knowledge of current records and information management practices.
- Working knowledge of privacy and information management legislations and guidelines.
- High level of proficiency with Microsoft Office software (particularly Teams, Excel, Outlook, Word, Planner, To Do and PowerPoint).
- Basic knowledge of the Microsoft Power Platform (Power Apps, Power Automate, Power BI).
- Strong written and verbal communications skills.
- Ability to provide oversight and guidance to other staff.
- Ability to lift boxes up to 20lbs.
- Ability to logically analyze, categorize and systemize complex information.

SENIOR MANAGER, INFORMATION SERVICES

SUMMARY

The Senior Manager, Information Services provides leadership and oversight to the information technology (IT) and business systems departments, including overseeing IT resources and systems, business systems applications, records management and privacy. This position reports to the Executive Director, Finance & Operations.

KEY ACCOUNTABILITIES

1. Responsible for Information Technologies, Business Applications, and Communications Systems.

- Conducts organization IT and communication systems strategic planning, through consultation with the Trust's Executive Management Committee and department directors and/or managers.
- Ensures reliable and robust performance and security of IT infrastructure systems and business applications.
- Manages the evaluation, selection, implementation and maintenance of information technology, business application and communication systems.
- Develops, maintains and communicates standards, policies, and procedures to ensure the protection and security of IT assets and the integrity, security and privacy of information entrusted to or maintained by the Trust.
- Develops and maintains an organization wide IT and business services recovery plan including mitigation plans to ensure timely and effective restoration of IT and communication services in the event of a disaster.
- Develops and maintains capital and operating budgets for the information and communications technology, business systems and records management functions and reports regularly on expenditure performance.
- Manages all outsourced IT third party and business partner relationships, including procurement and ongoing monitoring and managing to the contract and service agreements.
- Manages any IT Services required under the Asset Management Services Agreement with Columbia Power Corporation.

2. Oversees Corporate Records management.

- Maintains and advances the Trust's Records Management Program using organizational best practices and ensures that corporate records are stored, retrieved, provided and disposed of in accordance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and other applicable regulations.
- Oversees external requests and manages internal responses under FOIPPA, as the organizational Privacy Officer.
- Provides information about the Trust to external agencies as required to support business processes and in response to appropriate requests under FOIPPA.

3. Provides leadership and guidance to direct reports.

- Conducts performance evaluations.
- Provides coaching to enhance performance.
- Schedules staff resources as appropriate.

QUALIFICATIONS

Training and Experience

- A minimum of a Bachelor's Degree in Computer Science, Business Management or a related discipline OR an equivalent combination of education, training and experience.
- A minimum of eight years in computer systems and technology based work.
- Excellent knowledge of systems analysis, systems design, information technology, and communications technology.
- Experience in business continuity planning and records management.
- Experience in financial administration, planning and budgeting, and staff management.

Knowledge, Skills and Abilities

- Maintenance of up-to-date knowledge in operations areas, technological and communication trends through extensive reading and continued training.
- Sound knowledge of the Trust's objectives, operations and administrative and organizational structures.
- Sound knowledge of organizational effectiveness and operations management best practices.
- Working knowledge of record storage and maintenance practices and the *Freedom of Information and Protection of Privacy Act*.
- Sound knowledge of disaster recovery and business continuity planning.
- Extensive computer literacy including proficiency with all versions of MS Office.
- Strong interpersonal skills including skills in leadership, team-building and day-to-day supervision to create and maintain a positive working environment that supports staff in productive work outcomes and professional development.
- Strong commitment to customer service and the ability to instill this culture in the entire IT department.
- Ability to establish and maintain strong working relationships and to deal effectively with individuals inside and outside of the organization in a variety of consultative and collaborative processes that may be departmental or organization wide.
- Ability to clearly express and present views, ideas and facts effectively both orally and in writing.
- Ability to exercise initiative and bring sound independent judgment to resolving complex issues.
- Ability to prioritize and manage multiple projects while ensuring accuracy and meeting deadlines.
- Ability to maintain a high degree of confidentiality.

HR & Corporate Service Procedures

PROCEDURE TITLE: Freedom of
Information Requests

EFFECTIVE DATE: 2020-09

VERSION: 00

REVISED: XX

PURPOSE: This procedure details steps when Columbia Basin Trust (the Trust) or Columbia Power Corporation (CPC) receives a Freedom of Information (FOI) request to ensure compliance with the [Freedom of Information and Protection of Privacy Act, Chapter 165](#) and the [Province of British Columbia's](#) FOIPPA requirements.

RESPONSIBILITY:

Columbia Basin Trust Records and Information Management Coordinator (RM Coordinator).

All staff provide support and guidance to FOI request responses when needed.

PROCEDURE:

1. FOI Request is submitted to the RM Coordinator by the Applicant (or forwarded from another employee) outlining the request.
2. RM Coordinator reviews the request for legible and accurate information being requested. Ensure the FOI scope being requested is narrowed down to avoid extra efforts not needed. If the scope is not clear, contact the Applicant for further information.
3. Create a new FOI folder for The Trust [here](#) or CPC [here](#).
4. Update the Internal Request Tracking spreadsheet for The Trust [here](#) or CPC [here](#).
5. Reply to applicant with acknowledgement email confirming receipt of request.
6. RM Coordinator advises FOI request to Senior Manager, Information Services, CEO, and relevant Department Head.
7. If request does not fall within our organization:

- i. Send an email to applicant regarding denial of request as per Section 11 of the Act or transferring of the request as per Division 1 section 11.
- 8.** RM Coordinator with support from staff will gather and review the requested information according to FOIPPA:
 - a. 30 days to respond to applicant.
 - b. Consult with other public bodies associated with the request:
 - i. Information is redacted according to Division 2 of the Act (if required).
 - ii. Information relating to a public body is gathered and sent via email for consultation. This begins the process as outlined Division 3 of the Act.
 - iii. Response received from public body and CPC decides how to proceed.
 - iv. Information is sent to lawyer for review (if required).
 - c. Consult with third parties associated with the request:
 - i. Information is redacted according to Division 2 of the Act (if required).
 - ii. Information relating to a third party is gathered and via email for consultation. This begins the process as outlined Division 3 of the Act.
 - iii. Information is sent to lawyer for review (if required).
- 9.** If extension is required:
 - a. Email is sent to the requestor with the extension details as per Section 10 of the Act.
 - b. Information is redacted according to Division 2 of the Act (if required).
 - c. Information is sent to lawyer for review (if required).
- 10.** Final release package is prepared:
 - a. Circulate Final Letter to Senior Manager, Information Services, CEO, and relevant Department Head
 - b. Review and release final letter to Applicant
- 11.** Retain of all information electronically in the case file for The Trust [here](#) and CPC [here](#) to be managed as per The Trust's classification and retention schedule and Columbia Power's ARCS retention schedule.

ADDITIONAL RESOURCES:

Chief Information Officer's Privacy and Access Helpline (250-356-1851) or
Privacy.Helpline@gov.bc.ca

[Freedom of Information and Protection of Privacy Act: Regulation](#)

[Guidelines for the Determination of Fees Estimate](#)

[Ministry of Technology, Innovation and Citizens' Services: FOIPPA Policy and Procedures Manual](#)

[Ministry of Technology, Innovation and Citizens' Services: Non-Ministry Public Body Response Letters](#)

[Office of the Information & Privacy Commissioner: Forms, navigate to *Public Bodies*](#)

[Office of the Information & Privacy Commissioner for Public Bodies](#)

FOIPPA Quick Reference Guide

This Quick Reference Guide is intended to provide staff with immediate access to key points associated with the *Freedom of Information and Protection of Privacy Act* (FOIPPA) * of BC.

1. All records in the custody, or under the control of the Trust and Columbia Power Corp (the organizations) are subject to FOIPPA.
2. Records in the custody of a contractor, delivery partner, or service provider, and under the control of the organizations, are subject to FOIPPA.
3. All records are subject to access requests under FOIPPA (including relevant transitory* records that exist at the time of the request).
4. Many of the organizations' records are routinely available to the public, proactively provided, and do not require a formal FOI request.
5. Staff should accommodate reasonable access requests to non-confidential and non-personal information ***in an informal way*** wherever possible.
6. Requests for access to another person's personal information or to any confidential information are subject to exceptions in FOIPPA. The Privacy Officer (Senior Manager, Information Services) must be contacted if a formal request for records in writing has been made - privacy@ourtrust.org
7. The organizations have a ***duty to assist*** FOI applicants and must respond to formal FOI requests within 30 business days.
8. Personal information refers to "recorded information about an identifiable individual" and does not include business contact information*.
9. The organizations must only collect personal information if it ***is necessary to fulfill identified purposes and be reasonable and appropriate.***
10. Personal information collected may only be used for the purposes identified when it was collected.
11. An approved collection statement ***must be included*** on forms whenever personal information is being collected by the organizations or by delivery partners.
12. The organizations must make reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, or disposal of personal information.
13. A Privacy Impact Assessment (PIA) ***must be conducted*** on a new initiative, or before implementing a significant change to an existing initiative.
14. A completed corporate PIA covers the use of our in-house grant and program application system.
15. Any suspected or known privacy breach must be reported to the Privacy Officer immediately – privacy@ourtrust.org.

* Additional information is provided under the Privacy section of the Intranet:
https://ourtrust.sharepoint.com/departments/infoservices/Pages/rm_privacy.aspx

Intranet Screen Shots – Staff Information and Procedures

Records Management and Privacy

As Crown corporations, both the Trust and Columbia Power have regulatory responsibilities that are similar but differ in regards to records management and privacy.

As part of the Shared Services transition the Records Management and Privacy team will be reviewing opportunities to standardize related policies and procedures over time to reduce staff effort while ensuring appropriate compliancy remains in effect. Please see below for information and resources relevant to both corporations.

TRUST		CPC
Records Management	Has a records management policy, program and custom developed classification system.	Must comply with the Information Management Act and utilizes the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS).
Privacy	As a public body both corporations must comply with the Freedom of Information and Protection of Privacy Act (FOIPPA) .	

Privacy Impact Assessments (PIA)

A PIA is a risk management process that we follow to protect the personal information we collect. Section 69 (5.3) of FOIPPA requires the Trust to conduct PIA's for all current or proposed initiatives.

Business units are required to do a PIA as part of the development phase of a proposed initiative (systems, projects, programs or activities), and if an initiative materially changes.

Where to start? Head to our ***NEW*** PIA flowchart [here](#) where you'll navigate through our new process.

If you know that you're not using our in-house Online Applications or form system, and/or information/data will be flowing to a third part or external system...complete the [Pre-PIA](#) form and submit for the Privacy Officer's review.

Some examples that require PIA's are as follows:

- Intake
- DOB Program
- Initiative
- Software or platform
- Policies
- And much much more

Still have questions? Connect with privacy@ourtrust.org.

Privacy Resources

2021 FOIPPA Training	PowerPoint presentation of privacy training session provided to staff.
Trust FOIPPA Manual	Designed to provide staff with an overview of FOIPPA and its application to the records of Columbia Basin Trust (CBT).
Quick Reference Guide	Immediate access to key points associated with administering the FOIPPA Manual and protecting privacy.
PIA Flowchart	Navigate the PIA process and determine what action is needed based on your program or initiative.
Pre-PIA Form	If your program or initiative is not using our in-house Online Applications or form system, and/or information/data will be flowing to a third part or external system...complete the form and submit for the Privacy Officer's review.
privacy@ourtrust.org	Please direct all questions regarding the Act, or Trust policies with respect to the release of information to this email. Also, if you receive an information request from the public, please reach out to us for support.

Key Terms

CONTACT INFORMATION	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." In other words, information that is used on business cards is contact information and does not constitute "personal information."
PERSONAL INFORMATION	<p>Personal information is simply defined as "recorded information about an identifiable individual other than contact information." Examples of personal information that may be withheld by the Trust includes, but is not limited, to the following:</p> <ul style="list-style-type: none">• An individual's name, home address, personal e-mail or telephone number.• An identifying number, symbol or other particular assigned to the individual (i.e. Social Insurance Number, driver's license number, database ID, etc.)• Information about the individual's education, financial, criminal or employment history.• Information about the individual's health care history, including a physical or mental disability.• Anyone else's opinion about the individual, but not the identity of the opinion holder. You can know what is said about you, but not who said it.• Images of identifiable individuals captured by cameras or surveillance systems.

RECORD	<p>A "record" is defined broadly under FOIPPA as any recorded information:</p> <p>"includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records."</p> <p>Records include letters, reports, e-mails, maps, calendars, post-it notes, annotations, doodles, database records, saved voice mail messages, etc. The information contained in records could be produced by the Trust or received from other sources, such delivery partners or other public bodies.</p> <p>If it is recorded, it is a record which may be subject to release under FOIPPA.</p>
---------------	---

Privacy FAQ's

<p>Q: For grants, the online form includes a declaration statement, but do I still need to complete a PIA?</p>	<p>A: No, our online form system has been pre-assessed by the Privacy department and any grants do not require a new PIA.</p>
---	--

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Procedures Manual

Updated September 12, 2017

Table of Contents

1. INTRODUCTION.....	4
2. THE <i>FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT</i>.....	5
Freedom of Information	5
Protection of Privacy	6
Key Definitions	6
Contact Information	6
Personal Information	6
Record	7
Records Management and FOIPPA	7
3. ROUTINELY AVAILABLE RECORDS	8
4. HANDLING REQUESTS FOR INFORMATION	9
Making a Request	9
Key Points to Remember	9
FOI Request Process Diagram.....	10
Requests for Personal Information	10
Requests for Correction of Personal Information	11
Timelines.....	11
Charging Fees.....	11
5. CORPORATE PRACTICES AND PROCEDURES.....	12
Agreements and Contracts	12
Application Forms	12
Board Meeting Records.....	12
Contractor Records	12
Delivery of Benefit Program Records	12
E-Mail.....	13
Employee Files.....	13
Grant Recipients	13
Invoices from Lawyers.....	14
List of Qualified Consultants.....	14
Police Investigations.....	14
Scholarship Recipients.....	14
Tenders.....	14

6. MANAGING PERSONAL INFORMATION	15
Collection of Personal Information.....	15
CBT Collection Statement	15
Forms and Survey Design.....	16
Internet-based Surveys	17
Use of Personal Information	17
Disclosure of Personal Information.....	17
Security of Personal Information	18
Retention of Personal Information	18
Keeping Information Current	19
7. PRIVACY IMPACT ASSESSMENTS.....	19
Elements of a PIA	19
PIA and Delivery Partners	20
Data Linking Regulations	20
Ceridian Canada Payroll System.....	22
Great Plains (Dynamics GP) Accounting System	22
Employee Files.....	22
IMS (Information Management System)	23
Payroll Files	23
Photo/Video/Audio Consent Forms	23
Records Database	24
9. ADDITIONAL RESOURCES	24
APPENDIX A – TABLE OF ROUTINELY AVAILABLE RECORDS.....	25
APPENDIX B – IDENTIFYING OFFICIAL AND TRANSITORY RECORDS	28
APPENDIX C – SAMPLE FOI REQUEST FORM.....	33
APPENDIX D – PRIVACY IMPACT ASSESSMENT TEMPLATE	35
APPENDIX E - PROTECTING SENSITIVE INFORMATION OUTSIDE THE OFFICE	36

1. INTRODUCTION

This procedures manual is designed to provide staff with an overview of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and its application to the records of Columbia Basin Trust (CBT).

The Head for the purposes of the Act is CBT's Chief Executive Officer and President. Any questions regarding the Act, or CBT policies with respect to the release of information, may be directed to Senior Manager, Information Services or to the FOI Coordinator.

Dwayne Lau
Senior Manager,
Information Services
Phone: 250.365.6633
E-mail: dlau@cbt.org

Nancy Boucher
Administrative Assistant & Records
FOI Coordinator
Phone: 250.304.1628
E-mail: nboucher@cbt.org

2. THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA) applies to all public bodies within the Province and has been in effect since 1994. "Public bodies" include ministries, local governments, schools and universities, crown corporations, hospitals, municipal police forces, and more as outlined in Schedule 2 of the Act.

Various access and privacy legislation has been enacted in Canada and applies to different jurisdictions. The following table illustrates the context of existing Canadian legislation for public and private sectors within federal and British Columbia jurisdictions:

Jurisdiction	Public sector	Private sector
Federal	Access to Information Act (AIA) Privacy Act (PA) (e.g. federal government departments, RCMP)	Personal Information Protection and Electronic Documents Act (PIPEDA) (e.g. banking institutions)
BC	Freedom of Information and Protection of Privacy Act (FOIPPA) (e.g. CBT)	Personal Information Protection Act (PIPA) (e.g. businesses, non-profit organizations)

FOIPPA represents the provincial government's legislative commitment to make public bodies more accountable and to protect personal privacy. FOIPPA gives individuals rights to access information held by public bodies (Freedom of Information) and protects their privacy by placing restrictions on local governments when collecting or disclosing personal information (Protection of Privacy). This means that there is a legislated set of rules governing what information can and cannot be released.

The underlying principle is that all recorded information is available to the public, except for information that is subject to the specific and limited exemptions to disclosure set out in Part 2 of the Act. FOIPPA does not replace other procedures for access, or limit access to information other than personal information, that is currently available to the public. Staff are expected to incorporate the concepts and procedures of the legislation into their regular business activities.

FREEDOM OF INFORMATION

FOIPPA establishes a process by which any person may request access to records held by CBT and other public bodies within the province. Individuals also have the right to review their own personal

information held by CBT.

The general right of access to information is restricted by certain specified and limited exceptions, which are necessary to protect a variety of needs of confidentiality and the right of individuals to privacy.

FOIPPA also provides a review process whereby decisions relating to the disclosure or non-disclosure of information and other related issues, may be reviewed by the Office of the Information and Privacy Commissioner for British Columbia.

Individuals requesting answers to questions (rather than requesting copies of records) will not typically be treated as an access for information request under the Act. Staff are expected to assist such individuals through routine departmental procedures as much as possible.

PROTECTION OF PRIVACY

FOIPPA protects the personal privacy of individuals by restricting the collection, use and disclosure of personal information. Disclosure of personal information, even to other public bodies, is strictly limited under Part 3 of the Act.

CBT may only collect personal information:

- That it has the authority to collect, or
- Where collection is directly related to and is necessary for operating a program.

Personal information can be used only for the purpose(s) for which it was originally obtained. The Act restricts multiple, inconsistent uses of information that was collected only once.

The individual from whom the information is collected is entitled to know what the information will be used for, and under what authority it is being collected.

As a rule of thumb, if you don't need personal information, don't collect it.

KEY DEFINITIONS

CONTACT INFORMATION

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." In other words, information that is used on business cards is contact information and does not constitute "personal information."

PERSONAL INFORMATION

Personal information is simply defined as "recorded information about an identifiable individual other

than contact information.” Examples of personal information that may be withheld by CBT includes, but is not limited, to the following:

- An individual's name, home address, personal e-mail or telephone number.
- An identifying number, symbol or other particular assigned to the individual (i.e. Social Insurance Number, driver's licence number, database ID, etc.)
- Information about the individual's education, financial, criminal or employment history.
- Information about the individual's health care history, including a physical or mental disability.
- Anyone else's opinion about the individual, but not the identity of the opinion holder. You can know what is said about you, but not who said it.
- Images of identifiable individuals captured by cameras or surveillance systems.

RECORD

A “record” is defined broadly under FOIPPA as any recorded information:

“includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.”

Records include letters, reports, e-mails, maps, calendars, post-it notes, annotations, doodles, database records, saved voice mail messages, etc. The information contained in records could be produced by CBT or received from other sources, such delivery partners or other public bodies.

If it is recorded, it is a record which may be subject to release under FOIPPA.

This definition of a record varies greatly to that used in Records Management, which distinguishes “official” records from “transitory” records. By regularly deleting or destroying records that have limited or no value to CBT operations, fewer records are stored that may respond to a formal request. Ultimately, this translates to greater cost savings to CBT in terms of storage space and staff time required to manage records and process FOI requests. Refer to Appendix C for more information on distinguishing official records from transitory ones.

It is also important to note that all records created or received during the regular conduct of business are CBT records and do not belong to the staff member who actually created or received them. CBT retains ownership of all records, even those created by a third party according to Contribution Agreements or Service Agreements.

RECORDS MANAGEMENT AND FOIPPA

FOIPPA imposes an expectation on public bodies to efficiently manage their recorded information

in a way that promotes transparency and openness. In some cases, the Act dictates a new approach to the collection, use, and disclosure of information. As a result, records management practices have a direct effect on how well CBT can comprehensively and efficiently respond to access requests.

CBT will be developing a corporate-wide Records and Information Management Program in the near future which will include the adoption of a standardized records classification system and retention schedule. The records classification system will be used by all departments to categorize CBT records in a consistent manner, enabling staff to quickly and easily search for and retrieve records throughout the organization, while decreasing the search time involved with responding to FOI requests.

By destroying records in accordance with the retention schedule, departments will further decrease the amount of time required to respond to FOI request since fewer records will be located in the department. Records are only to be destroyed in accordance with the corporate retention schedule.

If CBT receives a request for records that have been prepared for destruction, but have not yet been destroyed, the records are “frozen” until the request has been completed. This means that the records, if they apply to a request, must be included in response to the request.

3. ROUTINELY AVAILABLE RECORDS

Section 71 of the Act requires CBT to establish categories of records that are available to the public without a formal request for access.

The list below identifies common record types at CBT that are routinely available to the public. The list can be used to help staff determine whether or not a particular record can be released routinely or whether a more formal request is required. A comprehensive listing of CBT record categories is provided in Appendix A.

Examples of routinely available records include:

- Annual Reports
- Brochures and other publications
- Budgets (approved)
- Board minutes (open meetings)
- Maps
- Policies, procedures, manuals (approved)
- Program information (general)
- Resolutions (open meetings)
- Statistical Information
- Website information

Any requests for records not available routinely must be made in writing and directed to the FOI Coordinator.

4. HANDLING REQUESTS FOR INFORMATION

MAKING A REQUEST

The public has the legislated right to request records under the custody or in the control of CBT, subject to limited and specific exemptions (as outlined in Part 2 of the Act).

Before a formal written request for a record is made it should be established that the record being requested is not routinely available. Refer to section 3 for more information.

Routine requests – are requests for information that is commonly available through routine channels. The information may be available on the CBT website, in publications, or simply available upon request. The request can be verbal and does not require the involvement of the FOI Coordinator.

Formal requests – are requests for records that are neither routinely available nor available through routine channels. Formal requests under the Act must be made in writing. A form for this purpose is available in Appendix C, but a letter, fax or e-mail is also acceptable. Formal requests are to be directed to the FOI Coordinator as soon as received as there is a deadline for responding.

Staff may direct an applicant to the FOI Coordinator for assistance with making a request. Wherever possible, staff should assist an applicant in preparing a written request. Assistance may include helping an applicant to define the request as specifically as possible.

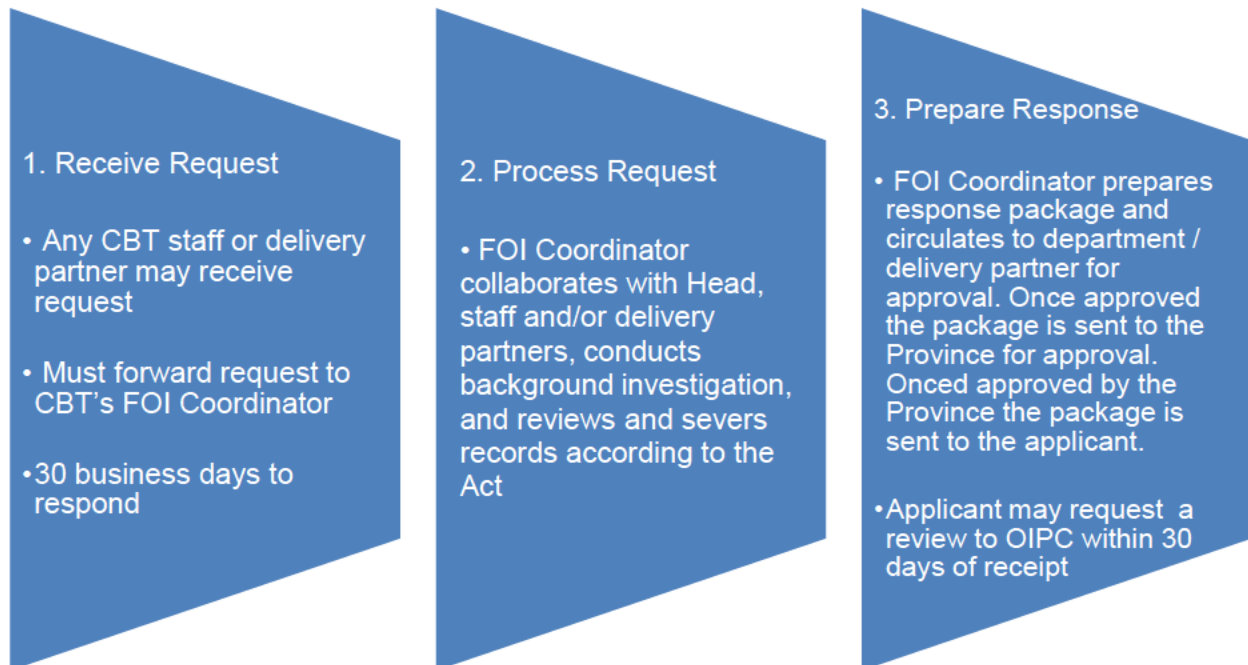
KEY POINTS TO REMEMBER

- Any staff member of any department can accept a written request for information.
- Requests can be in the form of a letter, e-mail, fax, or by using the form on the last page of this Manual, but must be made in writing.
- The Act does not apply to requests for answers to questions, only to requests for copies of or access to records.
- It is not necessary for applicants to quote the Act to obtain access to records.
- Duty to Assist – Section 6(1) of the Act requires CBT to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

- If records require severing before they can be disclosed, the request must be processed as a formal FOI request.

FOI REQUEST PROCESS DIAGRAM

The following diagram represents the standard process by which CBT handles formal requests for access to information:



REQUESTS FOR PERSONAL INFORMATION

FOIPPA guarantees an individual the right to see their own personal information held by CBT. The Act also restricts persons from getting access to personal information about another individual without the individual's consent.

Applicants may request access to their own personal information, either verbally or in writing.

Applicants who are requesting access to personal information belonging to a third party (i.e. not themselves), they may only obtain access by providing one of the following:

- The third party's signed consent for disclosure, or
- Proof of Authority to act on that person's behalf
 - e.g. Power of Attorney, Legal Representative

REQUESTS FOR CORRECTION OF PERSONAL INFORMATION

Incorrect personal information can have serious consequences for an individual. For example, incorrect personal information could result in the rejection of applications associated with available grants or scholarships, or the refusal of employment opportunities.

CBT must make every reasonable effort to ensure that personal information in their custody or control is accurate and complete. If someone's personal information changes, the person may make a request to CBT to correct the information in their files.

CBT must also provide the corrected information to any individual or company (i.e. delivery partner) to whom recorded information was disclosed within the preceding year. This means that a careful record must be kept of individuals and organizations to whom recorded personal information is disclosed.

Applicants may request the correction of their personal information, either verbally or in writing. CBT must correct or annotate the personal information as soon as possible.

TIMELINES

FOIPPA requires that a response be provided to the applicant within 30 days of receipt of the request. The term "day" is defined in the Act as "not including a holiday or a Saturday." In the *Interpretation Act*, the definition of "holiday" includes Sundays, and statutory holidays. The combined effect of these definitions is that weekends and holidays are not included in the calculation of time limits under FOIPPA and refer to "business" days.

Occasionally it might be necessary to extend the timeline by an additional 30 business days. Should this situation arise, the FOI Coordinator will advise the applicant of the time extension in advance.

CHARGING FEES

Section 75 of the *Freedom of Information and Protection of Privacy Act* permits public bodies to charge applicants fees for costs associated with processing request to access records through the Act. The maximum fees are set out in the *Freedom of Information and Protection of Privacy Regulation* (B.C. Reg. 155/2012) to the Act.

CBT will not charge fees associated with processing formal FOI requests.

5. CORPORATE PRACTICES AND PROCEDURES

The following are descriptions of existing CBT practices and procedures regarding some of the more frequent types of FOI requests. These practices reflect provisions of the Act as well as the corporate and administrative procedures of CBT. Please direct any questions to the Senior Manager, Information Services.

AGREEMENTS AND CONTRACTS

Care must be taken to examine the wording and clauses of an agreement or contract to ensure that it does not reveal trade secrets, proprietary information, or information which could possibly harm the business interests of a third party. Before releasing any contractual information, please check with the FOI Coordinator.

Wherever possible, contracts awarded by CBT should include a confidentiality clause stating the contract or agreement is subject to FOIPPA and may be released upon request. In addition, contracts and agreements should address whether CBT or the consultant/contractor has ownership of the records created while under contract. Staff are encouraged to contact the Senior Manager, Information Services for examples of appropriate wording.

APPLICATION FORMS

Completed application forms may contain personal information and third party business information that may be excepted from disclosure. All requests for completed application forms, even those held by CBT's delivery partners, must be handled as a formal request.

BOARD MEETING RECORDS

Board of Directors minutes for regular (open) meetings are posted to the CBT website and are routinely available after they have been approved by the Board at the following meeting.

CONTRACTOR RECORDS

Records that are created by contractors under a Service Agreement containing a Schedule F with CBT may be owned by CBT and could be subject to FOIPPA. Other contractor records are owned by the contractor and are subject to the BC *Personal Information Protection Act* (PIPA).

DELIVERY OF BENEFIT PROGRAM RECORDS

Records that are created or received by delivery partners under a Contribution Agreement with CBT may be owned by CBT and are subject to FOIPPA.

Other delivery partner records are owned by the delivery partner and are subject to the BC *Personal Information Protection Act* (PIPA) in the case of non-profit organizations and private companies, and FOIPPA in the case of public bodies.

Requests for Delivery of Benefit Program records must be processed by CBT's FOI Coordinator.

E-MAIL

If an e-mail contains information about CBT decisions, strategies, or transactions, it must be saved electronically or printed and retained in the relevant file. Junk mail and e-mail that does not contain information of value to CBT should be deleted on a regular basis. Staff are to refrain from forwarding CBT email to web-based email accounts, such as Gmail or Hotmail.

Please note that when you are requested by the Head or Coordinator to produce records in response to a request, it is expected that you will also include any relevant e-mail records in your possession.

EMPLOYEE FILES

Employees are entitled to view their employee file. A request in advance must be made to the Human Resources Coordinator to arrange a time to review the file. Direct supervisors may access employee files in order to review work history, education/training, discipline, etc.

Please note that as an employee, you are entitled to see any comments made about you – that is your personal information. However, the identity of the person making the comments may be withheld.

Information regarding a person's employment history is considered personal information and will not be disclosed to third parties, unless express permission of the employee is obtained first. This includes information regarding benefits paid to the employee. If a request for salary information is received, the requestor will be told of the salary range for that particular position without identifying any individual's specific salary unless express permission from the employee has been obtained first.

GRANT RECIPIENTS

The names of successful grant recipients are routinely released, in addition to the geographic location of the individual, monetary amount awarded, and the purpose of the grant (i.e. project title). Any additional personal information or sensitive business information supplied in support of the grant application will only be released according to the provisions of the Act.

INVOICES FROM LAWYERS

Requests for details of legal invoices must be forwarded to the FOI Coordinator. The details may divulge the strategy or grounds on which a legal case is being based or disclose personal information, therefore must be treated as a formal FOI request. Individual or case specific invoices are considered privileged communication between the solicitor and CBT and are usually withheld.

LIST OF QUALIFIED CONSULTANTS

CBT maintains a database of consultants within the Basin who have satisfactorily responded to published Requests for Qualifications. This list is used for internal purposes and will not be routinely released.

POLICE INVESTIGATIONS

Section 33.2(i) of the FOIPP Act states that public bodies can disclose information to law enforcement bodies in order to assist in a law investigation matter. Staff can provide the requested information directly to the RCMP, provided that sufficient identification is supplied by the officer.

CBT does not have jurisdiction over RCMP records and cannot transfer a request for RCMP records made under FOIPPA. Requests for RCMP records must be directed to the RCMP, as they are a federal body subject to the federal *Access of Information Act* and the federal *Privacy Act*.

SCHOLARSHIP RECIPIENTS

Similar to grant recipients, the name of scholarship recipients, the monetary value of the scholarship, geographic location and name of the school is routinely released. Any additional personal information supplied in support of the nomination or application will only be released according to the provisions of the Act.

TENDERS

Tenders submitted to CBT in response to Request for Proposals are available to the public, except for information regarding unit pricing, employment histories, and other confidential third party business information. The release of such information could potentially harm the company's business interests and personal information of their employees. Unit pricing information is considered proprietary information belonging to the third party and is "blacked out" or severed prior to disclosure.

It is recommended that all issued request for proposals contain a statement advising that “All proposals received may be made publicly available, except information relating to unit pricing, confidential third party business information, and employment history of the contractor and their employees.”

Requests for copies of tenders submitted to CBT must be directed to the FOI Coordinator.

6. MANAGING PERSONAL INFORMATION

FOIPPA governs how public bodies are to collect, use and retain personal information. It is our duty to ensure that information is legitimately collected, is stored securely, is kept current, and is used only for the purposes for which it is collected.

Individuals must be advised of what the information being gathered is going to be used for, and what authority CBT has for collecting that information.

COLLECTION OF PERSONAL INFORMATION

The Act imposes limitations on the collection of personal information. CBT may only collect personal information under the following circumstances:

- Where the collection is expressly authorized by law,
- For law enforcement purposes, or
- Where the information relates directly to, and is necessary for, an operating program or activity of the public body.

CBT needs to collect personal information when it is essential for program delivery or operational requirements. Methods of collection include forms, questionnaires, personal interviews, surveys, etc. Even unsolicited resumes from job applicants are considered to be “collected” by CBT if they are kept on file.

Staff should only collect personal information directly from the person concerned, wherever possible. Individuals must be advised of what the information being gathered is going to be used for, and what authority the local public body has for collecting that information.

CBT COLLECTION STATEMENT

Staff and delivery partners are encouraged to include the following collection statement on all forms that are used to collect personal information:

The personal information requested on this form is collected under the authority of section 26(c) of the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and will be used by Columbia Basin Trust for [administrative and evaluative purposes only]. The collection, use and disclosure of personal information is subject to the provisions of the FOIPPA and any questions regarding such may be directed to: FOIPPA Inquiries, Senior Manager, Information Services, Columbia Basin Trust, Suite 300, 445-13th Ave., Castlegar, BC, V1N 1G1, 1-800-505-8998.

FORMS AND SURVEY DESIGN

Prior to designing forms or surveys for hard copy distribution, it is important to examine their purpose, use and format. Whether online or in paper format, forms and surveys that collect personal information by CBT or by delivery partners on behalf of CBT must be designed to provide the public with the following necessary information:

1. How the personal information is to be used;
2. Under what authority CBT is collecting the personal information;
3. The name, position and telephone number of a staff member to whom questions may be directed.

For example, a grant application form may contain the following notification:

The personal information requested on this funding application is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FOIPPA) and will be used by Columbia Basin Trust (CBT) for administrative and evaluative purposes only. The collection, use and disclosure of personal information is subject to the provisions of the FOIPPA. Any questions regarding such may be directed to: FOIPPA Inquiries, Senior Manager, Information Services, Columbia Basin Trust, Suite 300, 445-13th Ave., Castlegar, BC, V1N 1G1, 1-800-505-8998.

A further clause must be added to funding applications to indicate that, as result of the application, some information will be routinely available to the public.

By submitting this funding application, you hereby acknowledge that CBT may disclose this application, and the information contained herein, including but not limited to your name, budget, location and the amount and nature of any related funding to the public, individuals or any other entity to the extent allowed by FOIPPA. You further agree that CBT may proactively disclose to the public your name, location, amount and nature of funding granted.

Moreover, it is important to regularly review forms and surveys that are used to collect personal information from individuals. To help ensure the minimum amount of personal information is being collected for a particular purpose, refer to the following questions:

- Do you need the information?
- Do you have authority to collect the information?
- What will the information be used for?

- Who else will you provide that information to?
- Is the applicant advised of what the information will be used for and under what authority?

INTERNET-BASED SURVEYS

In response to the Homeland Security Act and Patriot Act enacted in the United States, Section 30.1 of FOIPPA requires that all personal information is stored and accessed only in Canada, unless express consent is obtained from the individual for a specified purpose.

When conducting internet-based surveys, the personal information collected must reside on a server within Canada in accordance with section 30.1 of FOIPPA, unless participants expressly consent to their personal information residing outside of Canada for a specified purpose. Survey Monkey is a popular online survey application, however, it must be used carefully as all survey data is stored on servers located in the United States. Staff are encouraged to use Canadian internet-based surveys wherever possible, such as FluidSurveys or LimeSurvey,

USE OF PERSONAL INFORMATION

FOIPPA embodies the principle that individuals own their personal information and have the right to exercise control over its use and disclosure wherever it is held.

CBT is only permitted to use personal information for the following purposes:

- The purpose for which it was collected or a use consistent with that purpose,
- A purpose for which the person concerned has consented in writing, or
- A purpose for which the information may be disclosed to the public body under section 33 to 36 (see below).

DISCLOSURE OF PERSONAL INFORMATION

CBT is only permitted to disclose personal information in certain circumstances. The most common are as follows:

- In response to an FOI request,
- If the individual the information is about has consented in writing,
- For the purpose for which it was obtained or for a use consistent with that purpose,
- For the purpose of complying with a law of British Columbia or Canada,
- For the purpose of complying with a subpoena, warrant or court order,

- To an officer or employee of CBT if the information is necessary for the performance of his or her duties or safety (“need-to-know” principle),
- To a public body or a law enforcement agency in Canada to assist in a law enforcement matter, and
- For research, statistical, archival or historical purposes.

SECURITY OF PERSONAL INFORMATION

The security of personal information is one of the most important privacy-related issues that public bodies face. Reasonable security arrangements must be established and maintained to protect personal information against unauthorized access, collection, use, disclosure or disposal.

In response to the recent and significant privacy breach involving the University of Victoria, the Information and Privacy Commissioner has confirmed that “reasonable security arrangements” are not one-size-fits-all. They are dependent on a number of factors, such as determining:

- The level of sensitivity of the personal information,
- The medium and format of the records,
- Costs of security, and
- How valuable the information might be to those intending on misusing it.

It is recommended that all staff practice good privacy protection by:

- Using electronic passwords on their PCs and locking them when away from their work station or desk,
 - Keep passwords confidential
- Using passwords and encryption when storing and transmitting personal information via mobile devices (laptops, Blackberry cellular phones, USB sticks, etc.),
- Using locks on cabinets,
- Turning monitors away from public view, and
- Not leaving completed application forms and other records containing personal information in high traffic and/or public areas.

Please refer to the Information Technology Policies for additional information.

RETENTION OF PERSONAL INFORMATION

CBT is required to retain personal information for one year if that information was used as a basis for a decision directly affecting the individual but after the year it can be destroyed if in accordance with

the records retention schedule.

In general, personal information should be retained only as long as it is useful, and then be securely destroyed.

KEEPING INFORMATION CURRENT

Section 29 of the Act establishes control over personal information by giving an individual the right to request correction of her or his own personal information in the custody or control of a public body. A correction may involve a request to change personal information that is incorrect or to add updated personal information.

What this means is that if a person requests a change to their personal information, it is up to CBT to ensure that the change is made to the records within its custody and control, and to provide the change to any other body the information might have been provided to in the course of the service for which the information was collected.

As CBT receives personal information about funding recipients from delivery partners, it is likely that individuals will contact delivery partners rather than CBT for any corrections. In that case, delivery partners need to notify CBT of any changes to personal information.

7. PRIVACY IMPACT ASSESSMENTS

Section 69 (5.3) of FOIPPA requires CBT to conduct Privacy Impact Assessments (PIA) for all current or proposed initiatives (systems, projects, programs or activities) for the purpose of evaluating privacy impacts and to ensure compliance with privacy protection responsibilities under Part 3 of the Act. A PIA is both an educational tool and a collaborative process designed to support business objectives, including electronic initiatives. When used as part of normal business activities, a PIA can ensure that privacy requirements are identified and satisfied in a timely and cost efficient manner.

ELEMENTS OF A PIA

A Privacy Impact Assessment Template has been developed for CBT staff use (see Appendix D), and is designed to ensure all relevant privacy protection implications regarding the collection, protection, retention, use and disclosure of personal information have been identified and assessed.

Each PIA consists of the following elements:

1. General contact information for individual qualified to answer questions about the PIA
2. Description of the initiative

3. Purpose/objective of the initiative
4. Potential impacts of the proposal
5. Details of any previous PIAs or privacy assessments done on the initiative (in whole or in part)
6. Description of the elements of personal information that will be collected, used, and/or disclosed and the nature and sensitivity of the personal information
7. Description of the linkages and flows of personal information collected, used, and disclosed
8. Analysis of the FOIPPA authorities allowing collection, use, and/or disclosure for the initiative
9. Description of procedures in place to enable an individual to correct or annotate their personal information
10. Analysis of security and storage of personal information
11. Description of retention of personal information
12. PIA signed off by individuals with primary responsibility for privacy (and security where relevant) on the initiative

PIA AND DELIVERY PARTNERS

CBT may be responsible for the personal information in the custody or under the control of delivery partners engaged in CBT funded activities. CBT shall work with delivery partners to develop PIAs for CBT funded program as required.

A PIA has been completed for the Basin Business Advisory Program, and may be used as a staff reference when developing future PIAs by contacting the Manager, Operations.

DATA LINKING REGULATIONS

One of the recent changes to FOIPPA enables the Provincial government to prescribe regulations related to data linking. To paraphrase the definition provided in the Act, data linking can be described as being “the linking or combining of personal information in one or more databases if the purpose of the linking or combining is different from the purpose for which the information in each database was originally obtained or compiled.”

An example of a “data-linking initiative” or “common or integrated program or activity” is the BC Services Card, which links driver’s license information with health care information, and may be used for additional purposes in the future. Such initiatives have profound privacy implications and require the involvement of the Office of the Information and Privacy Commissioner, in accordance with sections 69 (5.4) and 69 (5.5) of FOIPPA.

Should CBT plan to develop a program or initiative to link personal information held in multiple databases and will be utilized by one or more public bodies and one or more agencies, the Office of the Information and Privacy Commissioner must be notified at the conceptual stage of the project and a PIA must be provided for review and comment prior to development. CBT should

also check with the Ministry of Technology, Innovation and Citizens' Services to determine whether the government has prescribed any data linking regulations.

8. PERSONAL INFORMATION DIRECTORY

CBT is required under section 69(6) of the *Freedom of Information and Protection of Privacy Act* to make available for inspection and copying by the public a Personal Information Directory. This Directory must list each personal information bank (PIB) held by CBT and list the following for each:

1. Its title and location;
2. A description of the kind of personal information and the categories of individuals whose personal information is included;
3. The authority for collecting the personal information;
4. The purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed; and
5. The categories of persons who use the personal information or to whom it is disclosed.

The Act defines a "personal information bank" as:

a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

It should be noted that not all collections of personal information are considered personal information banks. The key to determining whether a group of files, which contain personal information, is a PIB is how they are arranged or retrieved. Collections of personal information that relate to an individual and are organized and retrievable by the person's last name or personal identifier are considered personal information banks. Collections of personal information that are organized and retrieved by an identifier that relates to a corporate body or other search field are *not* listed as personal information banks, even if the collections contain personal information.

PIB Checklist:

- Does the file bank contain personal information?
- Does the file bank contain like or similar personal information?
- Is the information linked to an identifiable individual?
- Is the information organized and capable of being retrieved by a personal identifier?

The following directory is organized alphabetically by existing PIB name, and will be updated as needed.

CERIDIAN CANADA PAYROLL SYSTEM

1. Employee payroll information is stored and retrieved electronically using the Ceridian server, which is located in Canada.
2. These records contain payroll information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for administering payroll activities.
5. Human Resources staff, supervisors, employees.

GREAT PLAINS (DYNAMICS GP) ACCOUNTING SYSTEM

1. Accounting information is stored and retrieved electronically using the Great Plains application, which is located on the internal CBT server at the Castlegar main office.
2. These records contain home addresses of committee members and individuals who have received reimbursements from CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (accounting activities).
4. The personal information is compiled and used for administering accounts payable and accounts receivable activities.
5. Finance staff, supervisors.

EMPLOYEE FILES

1. Employee files are located in the Human Resources Department and in the Semi-Active Records Storage room.
2. These files contain employment and benefit information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for employment-related purposes.

5. Human Resources staff, supervisors, employees.

IMS (INFORMATION MANAGEMENT SYSTEM)

1. Contract information and awards and bursary recipient information is stored and retrieved electronically using IMS application, which is located on the internal CBT server at the Castlegar main office.
2. These records contain home addresses of individuals with whom CBT has contracted, as well as home addresses of individuals who have received CBT scholarships and bursaries.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (financial administration activities).
4. The personal information is compiled and used for financial administration purposes.
5. Supervisors, employees.

PAYROLL FILES

1. Employee payroll files are located in the Finance Department and in the Semi-Active Records Storage room.
2. These files contain payroll information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for employment-related purposes.
5. Finance staff, Human Resources staff, supervisors, employees.

PHOTO/VIDEO/AUDIO CONSENT FORMS

1. Signed consent forms are located in the Semi-Active Records Storage room and on the CBT server in Castlegar.
2. These records contain the name and signature of individuals who attend a CBT event and consent to their image/voice to be used for CBT marketing purposes.

3. Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (marketing activities).
4. The personal information is compiled and used for marketing purposes.
5. Communications staff.

RECORDS DATABASE

1. Descriptive information of physical CBT semi-active files are stored and retrieved electronically using the Records Database, which is located on the internal CBT server at the Castlegar main office.
2. The database contains titles of active and semi-active hard copy files, including the names of individuals with whom CBT has contracted and current and former employees.
3. Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (recordkeeping activities).
4. The personal information is compiled and used for recordkeeping purposes.
5. Administrative staff, supervisors.

9. ADDITIONAL RESOURCES

Freedom of Information and Protection of Privacy Act

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

Office of the Information and Privacy Commissioner for British Columbia

<http://www.oipc.bc.ca/>

Ministry of Technology, Innovation and Citizens' Services

Freedom of Information and Protection of Privacy: Policy and Procedures Manual

http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page

Ministry of Technology, Innovation and Citizens' Services

Legislation, Privacy and Policy Branch

http://www.cio.gov.bc.ca/cio/priv_leg/lpp.page?

Ministry of Community Services

Freedom of Information and Protection of Privacy: Questions and Answers – Local Government Bodies (Updated September 2005)

<http://www.msar.gov.bc.ca/privacyaccess/main/LocalGovtQA.pdf>

Local Government Management Association of BC

Freedom of Information and Protection of Privacy Act Toolkit for Local Government Organizations (November 2012)

Available for purchase at <http://www.lgma.ca/>

APPENDIX A – TABLE OF ROUTINELY AVAILABLE RECORDS

The table below identifies common record types at CBT that are routinely available to the public. Should you receive requests for records that are not listed below, please contact the Senior Manager, Information Services Operations or FOI Coordinator.

SUBJECT HEADING
A
Acts and Legislation – General Information
Advertising – Articles, Postings, etc.
Agendas – Open Meetings (Board of Directors and Advisory/Board Committees)
Annual Reports
Application Forms – Blank
Application Forms – Completed
Appointments (Board of Directors and Board Committees)
B
BASINLink Newsletter
Board Committees – Open Meetings
Board of Directors – Appointments
Board of Directors – General Information
Board of Directors – Open Meetings (Agendas/Minutes)
Budgets – Annual Financial Report
Budgets – Operating – Final
C
Calendar of Events
Classifications – Jobs
Committees – Board – Agendas/Minutes – Open Meetings

SUBJECT HEADING
Corporate Governance – General Information
D
Delivery of Benefits Programs and Activities – General Information
E
Employee Classification
Environmental Programs – General Information
F
Financial Statements – Annual
Fire Inspection Reports (Buildings and Facilities)
Forms (various) – Blank
Funded Projects (List)
Funding and Program Information
G
Governance – General Information
Grants from CBT – General Information
H
I
Initiatives – General Information
Investments – General Information
J
Job Classifications
Job Descriptions
K
L
M
Media Releases
Minutes – Board of Directors and Various Committees – Open Meetings
Mission Statement
N
News Releases
Newsletters
Nominations – Board of Directors (appointed)
Nominations – Committees (appointed)
O
Operating Budgets – Final
Organizational Charts
P

SUBJECT HEADING
Policy and Procedures – Approved
Program Guides
Property Taxes Paid
Provisional Budget – Final
Publications
Q
Quotations – General Information
R
Reclassifications
Registration Forms – Completed
Remuneration – Board of Directors
Remuneration – Staff earning over \$75,000 per year
Report to Residents
Reports – Annual
Reports – Financial
Reports to Board of Directors – Open Meetings
Requests for Proposals/Quotations – General Information
Resolutions – Open Meetings
S
Salary Ranges – Job Descriptions
Signing Authorities (List)
Social Media Sites (i.e. Facebook, Twitter)
Speeches
Staff Reports – Open Meetings
Statistics
T
Tax Exemptions
Taxation Assessments
Taxes Paid
Tenders
Training and Development – General Information
U
V
W
Workshops – General Information
X, Y, Z
Youth Committee Members (List)



APPENDIX B – IDENTIFYING OFFICIAL AND TRANSITORY RECORDS

Each CBT employee must distinguish official business records from transitory records on a regular basis.

Transitory records are records in any form (paper, electronic, etc.) which are of short-term value and have no continuing administrative, operational, evidential, informational or archival value to the organization. Transitory records are defined as:

Records of temporary usefulness that are not an integral part of an administrative or operational records series, that are not regularly filed with a standard classification system, and that are only required for a limited period of time for the completion of an action or the preparation of an ongoing record. Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions.

Official records are records in any form which have been created, received and set aside during the regular conduct of business. Unlike transitory records, official records are of long-term value to CBT and have continuing administrative, operational, evidential, informational or archival value to the organization. All official records are to be maintained according to the corporate records management practices.

As a general rule, transitory records should be destroyed in an appropriate manner (i.e. shredded, recycled, deleted) once their usefulness has expired. The retention is “event driven” and not a fixed period of time; it may be as short as a few hours or as long as several days, weeks or months. Please note that some transitory records may be relevant to your work and should therefore be retained. See *Deciding Which Records Are Transitory* below for more information.

Examples of Transitory Records

Transitory records include, but are not limited, to the following examples:

- **Draft Documents and Working Materials**
Includes rough notes, research notes, and calculations used for the preparation of correspondence, reports, memoranda or other business records. May be disposed of once the final version of a document is complete and the master (original) filed.
 - **Note:** Not all drafts are transitory. In some cases, offices responsible for drafting legislation, legal documents, policy, budgets, standards, guidelines or procedures might need to track the evolution of the final product. These offices may need to keep various drafts, research and working materials in order to have a records of changes made and why.
- **Convenience or Reference Copies**
Records provided to you “for your information” (i.e. “cc” copies), which contain information that may be useful only for a brief period of time. Examples include:



- Routine notices or memos regarding holidays or special events circulated to all staff.
 - Print outs from databases, applications and the internet.
 - Issues that do not require your action.
- **Duplicate Copies**
Refers to exact copies of a record (photocopy, electronic copy, etc.) that have been created and retained only for the convenience of reference. Includes stocks of blank forms, internal information material, pamphlets, publications, etc., that have no further use to the organization.
- **E-mail**
Some e-mails are transitory records, whereas other are business records. If the e-mail meets the definition of a transitory record, then it can be deleted when no longer required. Otherwise, it is an official business record and must be managed accordingly.
- **External Publications**
Includes books, magazines, catalogues, directories, periodicals, pamphlets, brochures, journals, newspapers, and software documentation, whether printed or in electronic form, that are obtained from sources outside of the organization.
- **Outdated Lists**
Includes outdated address lists, distribution lists, membership lists, etc.
- **Transmission Documents**
Includes letters, fax cover sheets, e-mail message, routing slips, etc., that accompany documents but do not add value.

Deciding Which Records are Transitory

Determining whether a record is transitory depends on individual judgment of the value of the record. One employee could deem a record to be transitory while another considered it to be official, because the roles of the employees and their use of the information are different.

The key consideration is that if a record has only immediate or very short-term value to CBT and will not be required again after it is obsolete, you can dispose of it as soon as you are finished with it. But if the information in the record will have some future business, financial, legal, research or archival value to the organization, then you should retain and file it. If you are in doubt, keep the record.

Use the diagram below to help you identify records that are considered transitory and can be routinely destroyed (shredded, recycled, or deleted) as required.



Does the record (paper or electronic) provide evidence of a business activity, decision or transaction?

If No:

It is a Transitory Record and can be disposed of appropriately (deleted, recycled, or shredded)

If Yes:

Does it contain information that is only of immediate or short-term value?

Is it a duplicate copy?

Is it a draft that won't be of any value once the final document has been produced?

If Yes:

It is a Transitory Record and can be disposed of appropriately (deleted, recycled, or shredded).

If No:

Does it have future business, financial, legal, informational or archival value to CBT?

Does it provide evidence of compliance with accountability or other business requirements?

Is it needed to support business activities?

If Yes:

It is an **Official Record** and must be filed.

Comparison of Official and Transitory Records

Refer to this table for a quick reference to see if your records are official or transitory.

Official Records Maintain according to the Records Management Program	Transitory Records Destroy when no longer needed
<ul style="list-style-type: none"> • Advice, recommendations, and decisions, as well as background material • Policies, procedures, protocols, etc., as well as background material • Planning and budget records, as well as background material • Important telephone, e-mail, and face-to-face discussions • Contracts and other legal agreements, as well as background material • Proposed legislation and regulations, as well as background material • Proposed legislation and regulations, as well as background material • Work completed by consultants and others for the organization • All financial transactions • All records showing that services have been provided, or obligations have been incurred • All records that show that the organization's information systems have been maintained and are reliable 	<ul style="list-style-type: none"> • Temporary information, such as simple message, routing slips, and post-it notes • Duplicate copies of an official record that does not have comments written on it • Notes and rough drafts of letters, memos, reports, minutes, etc. Note: If the information contains major revisions or helps to show how the final document was created, the record should be retained • Publications from external sources, such as supply catalogues, brochures, magazines, etc. • Junk mail • Mass distribution notices, messages, and memos that do not directly affect your duties. If you send out the message, you should file it. • Outdated mailing lists, contact information, etc. • Unused forms, outdated business cards, brochures, etc.



Tips for Controlling Transitory Records

Here are some helpful tips for dealing with transitory records:

- Don't create unnecessary transitory records by downloading documents and distributing them as attachments. If possible, provide a link to the original web site instead.
- Discard duplicate print and electronic documents when you are sure the master (original) has been filed.
- Dispose of draft versions of documents and working materials that you don't need to keep when you are sure the final version has been distributed and the original filed.
- Securely destroy supplies of blank forms, letterhead/memo paper and business cards once they are obsolete.
- Discard routine, external publications once they have been circulated and/or you no longer need them, or once they are obsolete.
- Dispose of information with short-term value once you have acted on it.
- Dispose of advertising material and unsolicited mail as soon as you're finished with it.
- Review your e-mail messages regularly and delete transitory messages once they are obsolete.
- Erase voice mail messages after you listen to them; erase archived messages once you no longer need to save them.
- Shred transitory records containing confidential or sensitive information.

Key Points to Remember:

- A record that documents the evolution of a business decision or action is an official record, not a transitory record, and must be kept on file.
- Whether a record is transitory will depend on an individual's work requirements.
- Shred transitory records containing confidential or sensitive information.
- If in doubt, keep the record.



APPENDIX C – SAMPLE FOI REQUEST FORM

The following page contains a form that may be used printed and/or electronically distributed to the public for requesting CBT records that are not routinely available.

The form is provided for convenience and is not a requirement for submitting a formal request for access to records (i.e. FOI request). An applicant must submit a written request in any format (i.e. letter, e-mail, or by using the form).

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT REQUEST FOR ACCESS TO RECORDS

YOUR CONTACT INFORMATION		
LAST NAME	FIRST NAME	ORGANIZATION / BUSINESS NAME
MAILING ADDRESS		
DAY PHONE NO. ()	ALTERNATE PHONE NO. ()	E-MAIL ADDRESS (Optional)
DESCRIPTION OF RECORDS YOU ARE REQUESTING		
PROVIDE A DETAILED DESCRIPTION OF THE RECORDS YOU ARE REQUESTING, INCLUDING THE APPLICABLE TIME FRAME(S). <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>		



ARE YOU REQUESTING ACCESS TO ANOTHER PERSON'S PERSONAL INFORMATION? ☐YES ☐NO

IF YES, ATTACH EITHER: A) THAT PERSON'S SIGNED CONSENT FOR DISCLOSURE, OR
B)PROOF OF AUTHORITY TO ACT ON THAT PERSON'S BEHALF

PREFERRED METHOD OF
ACCESS TO RECORDS:

- ☐ EXAMINE ORIGINAL
- ☐ RECEIVE COPY – MAIL
- ☐ RECEIVE COPY – WILL PICK UP

YOUR SIGNATURE

DATE SIGNED
(DD/MM/YYYY)

PERSONAL INFORMATION CONTAINED ON THIS FORM IS COLLECTED UNDER SECTION 26(C) OF THE FREEDOM OF INFORMATION PROTECTION OF PRIVACY ACT AND WILL BE USED ONLY FOR THE PURPOSE OF RESPONDING TO YOUR REQUEST. FOR ASSISTANCE, CONTACT THE FOI COORDINATOR AT 250.304.1628.

APPENDIX D – PRIVACY IMPACT ASSESSMENT TEMPLATE

Please contact the Trust's Privacy Officer for the most recent version of the Privacy Impact assessment template.

APPENDIX E PROTECTING SENSITIVE INFORMATION OUTSIDE THE OFFICE

INTRODUCTION

To protect sensitive information, Trust employees must adhere to the following procedure when working in the field, from home or while travelling to protect paper and electronic records.

POLICIES

1. If you must take sensitive information with you, take only what you need and leave the rest behind. If possible, take copies and leave originals in the office.
2. Password-protect your electronic devices, plus any sensitive information you store on these devices. Use encryption, locks and alarms as appropriate.
3. Log off or shut down a device when not in use.
4. While away, keep devices and sensitive records with you at all times. For example, do not leave them in an unlocked office or meeting room, including during meals and other breaks.
5. If you must leave devices or records, place them in a secure location like a locked room or desk drawer. Consider storing them overnight at a local Trust office or in a hotel safe.
6. Only leave devices and records in a vehicle if there is no other option, and only if the vehicle is parked in a secure location for a brief period. Lock them in the trunk, not in plain view.
7. If working at home, store sensitive information in a locked filing cabinet or desk drawer that no one else can access. Avoid storing sensitive information on your home computer unless the information is encrypted and password-protected and the computer has security measures like anti-virus software and firewalls.
8. Avoid viewing or discussing sensitive information in public or while travelling. If you must do so, ensure no one can view or overhear the information.
9. Do not share work-designated devices with family members, friends and others.
10. Fax or photocopy sensitive information yourself, or have someone else do it only while you are present.
11. When you return to the office, return records to their original storage places as soon as possible and destroy the copies securely. Also store any sensitive notes you created in secure locations.
12. If sensitive information is stolen or lost, immediately notify your supervisor. If it is someone else's personal information that has been stolen or lost, immediately notify the Trust's privacy officer, and consider notifying the person affected and informing him or her that steps that are being taken to recover the information.



This Secure Shredding Services Agreement ("Agreement") between Iron Mountain Canada Corporation ("IM") and Columbia Basin Trust ("Customer") is effective as of July 4, 2008.

Customer: Address 445 - 13 Avenue
City Castlegar Province BC Postal Code V1N 1G1
Contact Name Diana Dorosz Phone 2503656633
Contact email ddorsz@cbt.org Fax 2503656670
IM: District Name Kelowna Customer ID K4188 SalesRep ID AF4
Name A. Faulkner

SERVICE DESCRIPTION AND PRICING

RECURRING PAPER SHREDDING SERVICES

☒ On-site (Mobile) ☐ Off-site
☐ Weekly ☐ Every 2 Weeks ☒ Every 4 Weeks

Unit Type	#	Price Per	Total
Secure Console	2	x \$ 32.50	= \$ 65.00
65-Gallon Bin		x \$	= \$
Total Per Service Visit ¹ = \$			
Container Drop-off Fee, per container = \$			
Implementation & Education Package = \$			
Employee Awareness Posters = \$			

¹Minimum charge per service visit: (On-site) \$ 65.00 (Off-site) \$

ONE TIME PAPER SHREDDING SERVICE (ON-BOARD)

☐ On-site (Mobile) ☐ Off-site

Unit Type	#	Price Per	Total
Pound		x \$	= \$
65-Gallon Bin		x \$	= \$
1.2cf Banker Bx		x \$ 8.75	= \$
Total Shredding = \$			
Additional Labor = \$			
Container Drop-off Fee, per container = \$			
Estimated Total ² = \$			

²Total is subject to actual service billings.

Minimum charge per service visit is \$ 65.00

ADDITIONAL SERVICES (All other services, not specifically listed, will be charged at IM's then current rates.)

- Additional charge for Unscheduled Service Visit: \$25/visit*
- Shredding of Standard 1.2 Cubic Foot Carton: \$8.75/1.2cf BB
- Additional Compliance & Education Packages: \$50 / package
- Additional Employee Awareness Posters: \$5 / poster

*Additional charge for remote locations may apply.

SERVICE NOTES (Describe container location, number of Packages and Posters, & any special instructions.)

2 security consoles to be delivered wk of July 7/08 for 1/4/w svc.

TERMS AND CONDITIONS

- Compliance with Contracts, Laws and Regulations.** Customer shall be responsible for, and warrant compliance with, all contractual restrictions and all applicable laws, rules and regulations, including but not limited to environmental laws and laws governing the confidentiality, retention and disposition of information contained in any materials delivered to IM. Customer is the owner or legal custodian of the materials. Customer shall reimburse IM for any reasonable costs, fees or expenses (including reasonable attorneys' fees) incurred by IM in litigation which IM becomes involved solely because it is shredding materials for Customer.
- Hazardous Substances.** Customer shall not deliver to IM any material considered toxic or dangerous or which is regulated under any federal or provincial law or regulation relating to hazardous materials.
- Limitation of Liability.** IM shall not be responsible or liable in any manner whatsoever for the contents of any item delivered to it for shredding, and shall have no liability for the shredding of materials pursuant to Customer's direction. IM's maximum liability for any and all claims arising with respect to any particular services performed hereunder shall not exceed the aggregate amount Customer paid for the particular service during the one (1) month preceding the event which gives rise to the claim. **IM'S LIABILITY SHALL BE LIMITED TO DIRECT DAMAGES, AND IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING TORT, CONTRACT, OR OTHERWISE, SHALL IM BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS) EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**
- Force Majeure.** Each party shall be excused from any delay or failure in performance under this Agreement for any period if and to the extent that such delay or failure is caused by acts of God, governmental actions, labor unrest, riots, unusual traffic delays or other causes beyond its control.
- Additional Services.** This Agreement sets forth the complete terms and conditions for paper secure shredding services only. In the event that any other services are provided under this Customer ID, such services shall be governed by the terms and conditions of IM's standard Customer Agreement for such services.
- Term and Payment.** The Agreement shall continue in effect for 30 days, with automatic renewal for successive 30 day terms, unless written notice of non-renewal is delivered by either party to the other. Prices are set forth above. After the first year, the prices shall be set forth in a separate schedule. Services are invoiced monthly and payment is due net 30 days. Late payment fee: 1.00% per month. Transportation surcharges may be applied and changed monthly without notice in accordance with the fuel surcharge policy located at www.ironmountain.com/fuelsurcharge.

CUSTOMER: Diana Dorosz, Columbia Basin Trust

Sign and date: Diana Dorosz July 4/08

Print Name and Title: Diana Dorosz Receptionist

IRON MOUNTAIN CANADA CORPORATION

Sign and date: Mackenzie Friarke 7/8/08

Print Name and Title: Mackenzie Friarke GM.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Procedures Manual

Updated March 1, 2024

Table of Contents

1. INTRODUCTION.....	4
2. THE <i>FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT</i>	5
Freedom of Information	5
Protection of Privacy	6
Key Definitions	6
Contact Information	6
Personal Information	6
Record	7
Records Management and FOIPPA	7
3. ROUTINELY AVAILABLE RECORDS	8
4. HANDLING REQUESTS FOR INFORMATION	9
Making a Request	9
Key Points to Remember	9
FOI Request Process Diagram.....	10
Requests for Personal Information	10
Requests for Correction of Personal Information	11
Timelines.....	11
Charging Fees.....	11
5. CORPORATE PRACTICES AND PROCEDURES.....	12
Agreements and Contracts.....	12
Application Forms	12
Board Meeting Records.....	12
Contractor Records	12
Delivery of Benefit Program Records	12
E-Mail.....	13
Employee Files.....	13
Grant Recipients	13
Invoices from Lawyers.....	14
List of Qualified Consultants.....	14
Police Investigations.....	14
Scholarship Recipients.....	14
Tenders.....	14

6. MANAGING PERSONAL INFORMATION	15
Collection of Personal Information	15
CBT Collection Statement	15
Forms and Survey Design	16
Internet-based Surveys	17
Use of Personal Information	17
Disclosure of Personal Information	17
Security of Personal Information	18
Retention of Personal Information	18
Keeping Information Current	19
7. PRIVACY IMPACT ASSESSMENTS.....	19
Elements of a PIA	19
PIA and Delivery Partners	20
Data Linking Regulations	20
Ceridian Canada Payroll System.....	22
Great Plains (Dynamics GP) Accounting System	22
Employee Files.....	22
IMS (Information Management System)	23
Payroll Files	23
Photo/Video/Audio Consent Forms	23
Records Database	24
9. ADDITIONAL RESOURCES	24
APPENDIX A – TABLE OF ROUTINELY AVAILABLE RECORDS.....	25
APPENDIX B – IDENTIFYING OFFICIAL AND TRANSITORY RECORDS	28
APPENDIX C – SAMPLE FOI REQUEST FORM.....	33
APPENDIX D – PRIVACY IMPACT ASSESSMENT TEMPLATE	35
APPENDIX E - PROTECTING SENSITIVE INFORMATION OUTSIDE THE OFFICE	36

1. INTRODUCTION

This procedures manual is designed to provide staff with an overview of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) and its application to the records of Columbia Basin Trust (CBT).

The Head for the purposes of the Act is CBT's Chief Executive Officer and President. Any questions regarding the Act, or CBT policies with respect to the release of information, may be directed to Manager, Business Systems.

Wendy Armstrong
Manager, Business Systems
Information Services
Phone: 250.304.3694
E-mail: warmstrong@ourtrust.org

2. THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

British Columbia's *Freedom of Information and Protection of Privacy Act* (FOIPPA) applies to all public bodies within the Province and has been in effect since 1994. "Public bodies" include ministries, local governments, schools and universities, crown corporations, hospitals, municipal police forces, and more as outlined in Schedule 2 of the Act.

Various access and privacy legislation has been enacted in Canada and applies to different jurisdictions. The following table illustrates the context of existing Canadian legislation for public and private sectors within federal and British Columbia jurisdictions:

Jurisdiction	Public sector	Private sector
Federal	Access to Information Act (AIA) Privacy Act (PA) (e.g. federal government departments, RCMP)	Personal Information Protection and Electronic Documents Act (PIPEDA) (e.g. banking institutions)
BC	Freedom of Information and Protection of Privacy Act (FOIPPA) (e.g. CBT)	Personal Information Protection Act (PIPA) (e.g. businesses, non-profit organizations)

FOIPPA represents the provincial government's legislative commitment to make public bodies more accountable and to protect personal privacy. FOIPPA gives individuals rights to access information held by public bodies (Freedom of Information) and protects their privacy by placing restrictions on local governments when collecting or disclosing personal information (Protection of Privacy). This means that there is a legislated set of rules governing what information can and cannot be released.

The underlying principle is that all recorded information is available to the public, except for information that is subject to the specific and limited exemptions to disclosure set out in Part 2 of the Act. FOIPPA does not replace other procedures for access, or limit access to information other than personal information, that is currently available to the public. Staff are expected to incorporate the concepts and procedures of the legislation into their regular business activities.

FREEDOM OF INFORMATION

FOIPPA establishes a process by which any person may request access to records held by CBT and other public bodies within the province. Individuals also have the right to review their own personal

information held by CBT.

The general right of access to information is restricted by certain specified and limited exceptions, which are necessary to protect a variety of needs of confidentiality and the right of individuals to privacy.

FOIPPA also provides a review process whereby decisions relating to the disclosure or non-disclosure of information and other related issues, may be reviewed by the Office of the Information and Privacy Commissioner for British Columbia.

Individuals requesting answers to questions (rather than requesting copies of records) will not typically be treated as an access for information request under the Act. Staff are expected to assist such individuals through routine departmental procedures as much as possible.

PROTECTION OF PRIVACY

FOIPPA protects the personal privacy of individuals by restricting the collection, use and disclosure of personal information. Disclosure of personal information, even to other public bodies, is strictly limited under Part 3 of the Act.

CBT may only collect personal information:

- That it has the authority to collect, or
- Where collection is directly related to and is necessary for operating a program.

Personal information can be used only for the purpose(s) for which it was originally obtained. The Act restricts multiple, inconsistent uses of information that was collected only once.

The individual from whom the information is collected is entitled to know what the information will be used for, and under what authority it is being collected.

As a rule of thumb, if you don't need personal information, don't collect it.

KEY DEFINITIONS

CONTACT INFORMATION

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." In other words, information that is used on business cards is contact information and does not constitute "personal information."

PERSONAL INFORMATION

Personal information is simply defined as "recorded information about an identifiable individual other

than contact information.” Examples of personal information that may be withheld by CBT includes, but is not limited, to the following:

- An individual's name, home address, personal e-mail or telephone number.
- An identifying number, symbol or other particular assigned to the individual (i.e. Social Insurance Number, driver's licence number, database ID, etc.)
- Information about the individual's education, financial, criminal or employment history.
- Information about the individual's health care history, including a physical or mental disability.
- Anyone else's opinion about the individual, but not the identity of the opinion holder. You can know what is said about you, but not who said it.
- Images of identifiable individuals captured by cameras or surveillance systems.

RECORD

A “record” is defined broadly under FOIPPA as any recorded information:

“includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.”

Records include letters, reports, e-mails, maps, calendars, post-it notes, annotations, doodles, database records, saved voice mail messages, etc. The information contained in records could be produced by CBT or received from other sources, such delivery partners or other public bodies.

If it is recorded, it is a record which may be subject to release under FOIPPA.

This definition of a record varies greatly to that used in Records Management, which distinguishes “official” records from “transitory” records. By regularly deleting or destroying records that have limited or no value to CBT operations, fewer records are stored that may respond to a formal request. Ultimately, this translates to greater cost savings to CBT in terms of storage space and staff time required to manage records and process FOI requests. Refer to Appendix C for more information on distinguishing official records from transitory ones.

It is also important to note that all records created or received during the regular conduct of business are CBT records and do not belong to the staff member who actually created or received them. CBT retains ownership of all records, even those created by a third party according to Contribution Agreements or Service Agreements.

RECORDS MANAGEMENT AND FOIPPA

FOIPPA imposes an expectation on public bodies to efficiently manage their recorded information

in a way that promotes transparency and openness. In some cases, the Act dictates a new approach to the collection, use, and disclosure of information. As a result, records management practices have a direct effect on how well CBT can comprehensively and efficiently respond to access requests.

CBT will be developing a corporate-wide Records and Information Management Program in the near future which will include the adoption of a standardized records classification system and retention schedule. The records classification system will be used by all departments to categorize CBT records in a consistent manner, enabling staff to quickly and easily search for and retrieve records throughout the organization, while decreasing the search time involved with responding to FOI requests.

By destroying records in accordance with the retention schedule, departments will further decrease the amount of time required to respond to FOI request since fewer records will be located in the department. Records are only to be destroyed in accordance with the corporate retention schedule.

If CBT receives a request for records that have been prepared for destruction, but have not yet been destroyed, the records are “frozen” until the request has been completed. This means that the records, if they apply to a request, must be included in response to the request.

3. ROUTINELY AVAILABLE RECORDS

Section 71 of the Act requires CBT to establish categories of records that are available to the public without a formal request for access.

The list below identifies common record types at CBT that are routinely available to the public. The list can be used to help staff determine whether or not a particular record can be released routinely or whether a more formal request is required. A comprehensive listing of CBT record categories is provided in Appendix A.

Examples of routinely available records include:

- Annual Reports
- Brochures and other publications
- Budgets (approved)
- Board minutes (open meetings)
- Maps
- Policies, procedures, manuals (approved)
- Program information (general)
- Resolutions (open meetings)
- Statistical Information
- Website information

Any requests for records not available routinely must be made in writing and directed to the FOI Coordinator.

4. HANDLING REQUESTS FOR INFORMATION

MAKING A REQUEST

The public has the legislated right to request records under the custody or in the control of CBT, subject to limited and specific exemptions (as outlined in Part 2 of the Act).

Before a formal written request for a record is made it should be established that the record being requested is not routinely available. Refer to section 3 for more information.

Routine requests – are requests for information that is commonly available through routine channels. The information may be available on the CBT website, in publications, or simply available upon request. The request can be verbal and does not require the involvement of the FOI Coordinator.

Formal requests – are requests for records that are neither routinely available nor available through routine channels. Formal requests under the Act must be made in writing. A form for this purpose is available in Appendix C, but a letter, fax or e-mail is also acceptable. Formal requests are to be directed to the FOI Coordinator as soon as received as there is a deadline for responding.

Staff may direct an applicant to the FOI Coordinator for assistance with making a request. Wherever possible, staff should assist an applicant in preparing a written request. Assistance may include helping an applicant to define the request as specifically as possible.

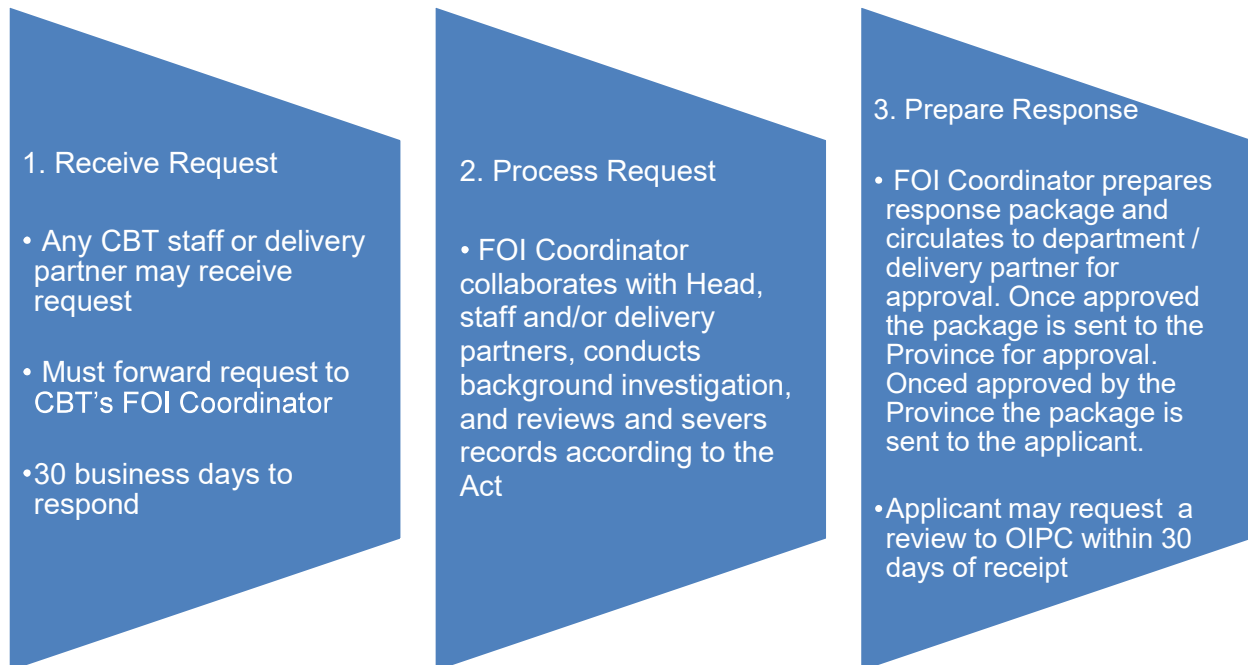
KEY POINTS TO REMEMBER

- Any staff member of any department can accept a written request for information.
- Requests can be in the form of a letter, e-mail, fax, or by using the form on the last page of this Manual, but must be made in writing.
- The Act does not apply to requests for answers to questions, only to requests for copies of or access to records.
- It is not necessary for applicants to quote the Act to obtain access to records.
- Duty to Assist – Section 6(1) of the Act requires CBT to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

- If records require severing before they can be disclosed, the request must be processed as a formal FOI request.

FOI REQUEST PROCESS DIAGRAM

The following diagram represents the standard process by which CBT handles formal requests for access to information:



REQUESTS FOR PERSONAL INFORMATION

FOIPPA guarantees an individual the right to see their own personal information held by CBT. The Act also restricts persons from getting access to personal information about another individual without the individual's consent.

Applicants may request access to their own personal information, either verbally or in writing.

Applicants who are requesting access to personal information belonging to a third party (i.e. not themselves), they may only obtain access by providing one of the following:

- The third party's signed consent for disclosure, or
- Proof of Authority to act on that person's behalf
 - e.g. Power of Attorney, Legal Representative

REQUESTS FOR CORRECTION OF PERSONAL INFORMATION

Incorrect personal information can have serious consequences for an individual. For example, incorrect personal information could result in the rejection of applications associated with available grants or scholarships, or the refusal of employment opportunities.

CBT must make every reasonable effort to ensure that personal information in their custody or control is accurate and complete. If someone's personal information changes, the person may make a request to CBT to correct the information in their files.

CBT must also provide the corrected information to any individual or company (i.e. delivery partner) to whom recorded information was disclosed within the preceding year. This means that a careful record must be kept of individuals and organizations to whom recorded personal information is disclosed.

Applicants may request the correction of their personal information, either verbally or in writing. CBT must correct or annotate the personal information as soon as possible.

TIMELINES

FOIPPA requires that a response be provided to the applicant within 30 days of receipt of the request. The term "day" is defined in the Act as "not including a holiday or a Saturday." In the *Interpretation Act*, the definition of "holiday" includes Sundays, and statutory holidays. The combined effect of these definitions is that weekends and holidays are not included in the calculation of time limits under FOIPPA and refer to "business" days.

Occasionally it might be necessary to extend the timeline by an additional 30 business days. Should this situation arise, the FOI Coordinator will advise the applicant of the time extension in advance.

CHARGING FEES

Section 75 of the *Freedom of Information and Protection of Privacy Act* permits public bodies to charge applicants fees for costs associated with processing request to access records through the Act. The maximum fees are set out in the *Freedom of Information and Protection of Privacy Regulation* (B.C. Reg. 155/2012) to the Act.

CBT will not charge fees associated with processing formal FOI requests.

5. CORPORATE PRACTICES AND PROCEDURES

The following are descriptions of existing CBT practices and procedures regarding some of the more frequent types of FOI requests. These practices reflect provisions of the Act as well as the corporate and administrative procedures of CBT. Please direct any questions to the Manager, Business Systems.

AGREEMENTS AND CONTRACTS

Care must be taken to examine the wording and clauses of an agreement or contract to ensure that it does not reveal trade secrets, proprietary information, or information which could possibly harm the business interests of a third party. Before releasing any contractual information, please check with the FOI Coordinator.

Wherever possible, contracts awarded by CBT should include a confidentiality clause stating the contract or agreement is subject to FOIPPA and may be released upon request. In addition, contracts and agreements should address whether CBT or the consultant/contractor has ownership of the records created while under contract. Staff are encouraged to contact the Manager, Business Systems for examples of appropriate wording.

APPLICATION FORMS

Completed application forms may contain personal information and third party business information that may be excepted from disclosure. All requests for completed application forms, even those held by CBT's delivery partners, must be handled as a formal request.

BOARD MEETING RECORDS

Board of Directors minutes for regular (open) meetings are posted to the CBT website and are routinely available after they have been approved by the Board at the following meeting.

CONTRACTOR RECORDS

Records that are created by contractors under a Service Agreement containing a Schedule F with CBT may be owned by CBT and could be subject to FOIPPA. Other contractor records are owned by the contractor and are subject to the BC *Personal Information Protection Act* (PIPA).

DELIVERY OF BENEFIT PROGRAM RECORDS

Records that are created or received by delivery partners under a Contribution Agreement with CBT may be owned by CBT and are subject to FOIPPA.

Other delivery partner records are owned by the delivery partner and are subject to the BC *Personal Information Protection Act* (PIPA) in the case of non-profit organizations and private companies, and FOIPPA in the case of public bodies.

Requests for Delivery of Benefit Program records must be processed by CBT's FOI Coordinator.

E-MAIL

If an e-mail contains information about CBT decisions, strategies, or transactions, it must be saved electronically or printed and retained in the relevant file. Junk mail and e-mail that does not contain information of value to CBT should be deleted on a regular basis. Staff are to refrain from forwarding CBT email to web-based email accounts, such as Gmail or Hotmail.

Please note that when you are requested by the Head or Coordinator to produce records in response to a request, it is expected that you will also include any relevant e-mail records in your possession.

EMPLOYEE FILES

Employees are entitled to view their employee file. A request in advance must be made to the Human Resources Coordinator to arrange a time to review the file. Direct supervisors may access employee files in order to review work history, education/training, discipline, etc.

Please note that as an employee, you are entitled to see any comments made about you – that is your personal information. However, the identity of the person making the comments may be withheld.

Information regarding a person's employment history is considered personal information and will not be disclosed to third parties, unless express permission of the employee is obtained first. This includes information regarding benefits paid to the employee. If a request for salary information is received, the requestor will be told of the salary range for that particular position without identifying any individual's specific salary unless express permission from the employee has been obtained first.

GRANT RECIPIENTS

The names of successful grant recipients are routinely released, in addition to the geographic location of the individual, monetary amount awarded, and the purpose of the grant (i.e. project title). Any additional personal information or sensitive business information supplied in support of the grant application will only be released according to the provisions of the Act.

INVOICES FROM LAWYERS

Requests for details of legal invoices must be forwarded to the FOI Coordinator. The details may divulge the strategy or grounds on which a legal case is being based or disclose personal information, therefore must be treated as a formal FOI request. Individual or case specific invoices are considered privileged communication between the solicitor and CBT and are usually withheld.

LIST OF QUALIFIED CONSULTANTS

CBT maintains a database of consultants within the Basin who have satisfactorily responded to published Requests for Qualifications. This list is used for internal purposes and will not be routinely released.

POLICE INVESTIGATIONS

Section 33.2(i) of the FOIPP Act states that public bodies can disclose information to law enforcement bodies in order to assist in a law investigation matter. Staff can provide the requested information directly to the RCMP, provided that sufficient identification is supplied by the officer.

CBT does not have jurisdiction over RCMP records and cannot transfer a request for RCMP records made under FOIPPA. Requests for RCMP records must be directed to the RCMP, as they are a federal body subject to the federal *Access of Information Act* and the federal *Privacy Act*.

SCHOLARSHIP RECIPIENTS

Similar to grant recipients, the name of scholarship recipients, the monetary value of the scholarship, geographic location and name of the school is routinely released. Any additional personal information supplied in support of the nomination or application will only be released according to the provisions of the Act.

TENDERS

Tenders submitted to CBT in response to Request for Proposals are available to the public, except for information regarding unit pricing, employment histories, and other confidential third party business information. The release of such information could potentially harm the company's business interests and personal information of their employees. Unit pricing information is considered proprietary information belonging to the third party and is "blacked out" or severed prior to disclosure.

It is recommended that all issued request for proposals contain a statement advising that “All proposals received may be made publicly available, except information relating to unit pricing, confidential third party business information, and employment history of the contractor and their employees.”

Requests for copies of tenders submitted to CBT must be directed to the FOI Coordinator.

6. MANAGING PERSONAL INFORMATION

FOIPPA governs how public bodies are to collect, use and retain personal information. It is our duty to ensure that information is legitimately collected, is stored securely, is kept current, and is used only for the purposes for which it is collected.

Individuals must be advised of what the information being gathered is going to be used for, and what authority CBT has for collecting that information.

COLLECTION OF PERSONAL INFORMATION

The Act imposes limitations on the collection of personal information. CBT may only collect personal information under the following circumstances:

- Where the collection is expressly authorized by law,
- For law enforcement purposes, or
- Where the information relates directly to, and is necessary for, an operating program or activity of the public body.

CBT needs to collect personal information when it is essential for program delivery or operational requirements. Methods of collection include forms, questionnaires, personal interviews, surveys, etc. Even unsolicited resumes from job applicants are considered to be “collected” by CBT if they are kept on file.

Staff should only collect personal information directly from the person concerned, wherever possible. Individuals must be advised of what the information being gathered is going to be used for, and what authority the local public body has for collecting that information.

CBT COLLECTION STATEMENT

Staff and delivery partners are encouraged to include the following collection statement on all forms that are used to collect personal information:

The personal information requested on this form is collected under the authority of section 26(c) of the *Freedom of Information and Protection of Privacy Act (FOIPPA)* and will be used by Columbia Basin Trust for [administrative and evaluative purposes only]. The collection, use and disclosure of personal information is subject to the provisions of the FOIPPA and any questions regarding such may be directed to: FOIPPA Inquiries, Manager, Business Systems, Columbia Basin Trust, Suite 300, 445-13th Ave., Castlegar, BC, V1N 1G1, 1-800-505-8998.

FORMS AND SURVEY DESIGN

Prior to designing forms or surveys for hard copy distribution, it is important to examine their purpose, use and format. Whether online or in paper format, forms and surveys that collect personal information by CBT or by delivery partners on behalf of CBT must be designed to provide the public with the following necessary information:

1. How the personal information is to be used;
2. Under what authority CBT is collecting the personal information;
3. The name, position and telephone number of a staff member to whom questions may be directed.

For example, a grant application form may contain the following notification:

The personal information requested on this funding application is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FOIPPA) and will be used by Columbia Basin Trust (CBT) for administrative and evaluative purposes only. The collection, use and disclosure of personal information is subject to the provisions of the FOIPPA. Any questions regarding such may be directed to: FOIPPA Inquiries, Manager, Business Systems, Columbia Basin Trust, Suite 300, 445-13th Ave., Castlegar, BC, V1N 1G1, 1-800-505-8998.

A further clause must be added to funding applications to indicate that, as result of the application, some information will be routinely available to the public.

By submitting this funding application, you hereby acknowledge that CBT may disclose this application, and the information contained herein, including but not limited to your name, budget, location and the amount and nature of any related funding to the public, individuals or any other entity to the extent allowed by FOIPPA. You further agree that CBT may proactively disclose to the public your name, location, amount and nature of funding granted.

Moreover, it is important to regularly review forms and surveys that are used to collect personal information from individuals. To help ensure the minimum amount of personal information is being collected for a particular purpose, refer to the following questions:

- Do you need the information?
- Do you have authority to collect the information?
- What will the information be used for?

- Who else will you provide that information to?
- Is the applicant advised of what the information will be used for and under what authority?

INTERNET-BASED SURVEYS

In response to the Homeland Security Act and Patriot Act enacted in the United States, Section 30.1 of FOIPPA requires that all personal information is stored and accessed only in Canada, unless express consent is obtained from the individual for a specified purpose.

When conducting internet-based surveys, the personal information collected must reside on a server within Canada in accordance with section 30.1 of FOIPPA, unless participants expressly consent to their personal information residing outside of Canada for a specified purpose. Survey Monkey is a popular online survey application, however, it must be used carefully as all survey data is stored on servers located in the United States. Staff are encouraged to use Canadian internet-based surveys wherever possible, such as FluidSurveys or LimeSurvey,

USE OF PERSONAL INFORMATION

FOIPPA embodies the principle that individuals own their personal information and have the right to exercise control over its use and disclosure wherever it is held.

CBT is only permitted to use personal information for the following purposes:

- The purpose for which it was collected or a use consistent with that purpose,
- A purpose for which the person concerned has consented in writing, or
- A purpose for which the information may be disclosed to the public body under section 33 to 36 (see below).

DISCLOSURE OF PERSONAL INFORMATION

CBT is only permitted to disclose personal information in certain circumstances. The most common are as follows:

- In response to an FOI request,
- If the individual the information is about has consented in writing,
- For the purpose for which it was obtained or for a use consistent with that purpose,
- For the purpose of complying with a law of British Columbia or Canada,
- For the purpose of complying with a subpoena, warrant or court order,

- To an officer or employee of CBT if the information is necessary for the performance of his or her duties or safety (“need-to-know” principle),
- To a public body or a law enforcement agency in Canada to assist in a law enforcement matter, and
- For research, statistical, archival or historical purposes.

SECURITY OF PERSONAL INFORMATION

The security of personal information is one of the most important privacy-related issues that public bodies face. Reasonable security arrangements must be established and maintained to protect personal information against unauthorized access, collection, use, disclosure or disposal.

In response to the recent and significant privacy breach involving the University of Victoria, the Information and Privacy Commissioner has confirmed that “reasonable security arrangements” are not one-size-fits-all. They are dependent on a number of factors, such as determining:

- The level of sensitivity of the personal information,
- The medium and format of the records,
- Costs of security, and
- How valuable the information might be to those intending on misusing it.

It is recommended that all staff practice good privacy protection by:

- Using electronic passwords on their PCs and locking them when away from their work station or desk,
 - Keep passwords confidential
- Using passwords and encryption when storing and transmitting personal information via mobile devices (laptops, Blackberry cellular phones, USB sticks, etc.),
- Using locks on cabinets,
- Turning monitors away from public view, and
- Not leaving completed application forms and other records containing personal information in high traffic and/or public areas.

Please refer to the Information Technology Policies for additional information.

RETENTION OF PERSONAL INFORMATION

CBT is required to retain personal information for one year if that information was used as a basis for a decision directly affecting the individual but after the year it can be destroyed if in accordance with

the records retention schedule.

In general, personal information should be retained only as long as it is useful, and then be securely destroyed.

KEEPING INFORMATION CURRENT

Section 29 of the Act establishes control over personal information by giving an individual the right to request correction of her or his own personal information in the custody or control of a public body. A correction may involve a request to change personal information that is incorrect or to add updated personal information.

What this means is that if a person requests a change to their personal information, it is up to CBT to ensure that the change is made to the records within its custody and control, and to provide the change to any other body the information might have been provided to in the course of the service for which the information was collected.

As CBT receives personal information about funding recipients from delivery partners, it is likely that individuals will contact delivery partners rather than CBT for any corrections. In that case, delivery partners need to notify CBT of any changes to personal information.

7. PRIVACY IMPACT ASSESSMENTS

Section 69 (5.3) of FOIPPA requires CBT to conduct Privacy Impact Assessments (PIA) for all current or proposed initiatives (systems, projects, programs or activities) for the purpose of evaluating privacy impacts and to ensure compliance with privacy protection responsibilities under Part 3 of the Act. A PIA is both an educational tool and a collaborative process designed to support business objectives, including electronic initiatives. When used as part of normal business activities, a PIA can ensure that privacy requirements are identified and satisfied in a timely and cost efficient manner.

ELEMENTS OF A PIA

A Privacy Impact Assessment Template has been developed for CBT staff use (see Appendix D), and is designed to ensure all relevant privacy protection implications regarding the collection, protection, retention, use and disclosure of personal information have been identified and assessed.

Each PIA consists of the following elements:

1. General contact information for individual qualified to answer questions about the PIA
2. Description of the initiative

3. Purpose/objective of the initiative
4. Potential impacts of the proposal
5. Details of any previous PIAs or privacy assessments done on the initiative (in whole or in part)
6. Description of the elements of personal information that will be collected, used, and/or disclosed and the nature and sensitivity of the personal information
7. Description of the linkages and flows of personal information collected, used, and disclosed
8. Analysis of the FOIPPA authorities allowing collection, use, and/or disclosure for the initiative
9. Description of procedures in place to enable an individual to correct or annotate their personal information
10. Analysis of security and storage of personal information
11. Description of retention of personal information
12. PIA signed off by individuals with primary responsibility for privacy (and security where relevant) on the initiative

PIA AND DELIVERY PARTNERS

CBT may be responsible for the personal information in the custody or under the control of delivery partners engaged in CBT funded activities. CBT shall work with delivery partners to develop PIAs for CBT funded program as required.

A PIA has been completed for the Basin Business Advisory Program, and may be used as a staff reference when developing future PIAs by contacting the Manager, Operations.

DATA LINKING REGULATIONS

One of the recent changes to FOIPPA enables the Provincial government to prescribe regulations related to data linking. To paraphrase the definition provided in the Act, data linking can be described as being “the linking or combining of personal information in one or more databases if the purpose of the linking or combining is different from the purpose for which the information in each database was originally obtained or compiled.”

An example of a “data-linking initiative” or “common or integrated program or activity” is the BC Services Card, which links driver’s license information with health care information, and may be used for additional purposes in the future. Such initiatives have profound privacy implications and require the involvement of the Office of the Information and Privacy Commissioner, in accordance with sections 69 (5.4) and 69 (5.5) of FOIPPA.

Should CBT plan to develop a program or initiative to link personal information held in multiple databases and will be utilized by one or more public bodies and one or more agencies, the Office of the Information and Privacy Commissioner must be notified at the conceptual stage of the project and a PIA must be provided for review and comment prior to development. CBT should

also check with the Ministry of Technology, Innovation and Citizens' Services to determine whether the government has prescribed any data linking regulations.

8. PERSONAL INFORMATION DIRECTORY

CBT is required under section 69(6) of the *Freedom of Information and Protection of Privacy Act* to make available for inspection and copying by the public a Personal Information Directory. This Directory must list each personal information bank (PIB) held by CBT and list the following for each:

1. Its title and location;
2. A description of the kind of personal information and the categories of individuals whose personal information is included;
3. The authority for collecting the personal information;
4. The purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed; and
5. The categories of persons who use the personal information or to whom it is disclosed.

The Act defines a "personal information bank" as:

a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

It should be noted that not all collections of personal information are considered personal information banks. The key to determining whether a group of files, which contain personal information, is a PIB is how they are arranged or retrieved. Collections of personal information that relate to an individual and are organized and retrievable by the person's last name or personal identifier are considered personal information banks. Collections of personal information that are organized and retrieved by an identifier that relates to a corporate body or other search field are *not* listed as personal information banks, even if the collections contain personal information.

PIB Checklist:

- Does the file bank contain personal information?
- Does the file bank contain like or similar personal information?
- Is the information linked to an identifiable individual?
- Is the information organized and capable of being retrieved by a personal identifier?

The following directory is organized alphabetically by existing PIB name, and will be updated as needed.

CERIDIAN CANADA PAYROLL SYSTEM

1. Employee payroll information is stored and retrieved electronically using the Ceridian server, which is located in Canada.
2. These records contain payroll information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for administering payroll activities.
5. Human Resources staff, supervisors, employees.

GREAT PLAINS (DYNAMICS GP) ACCOUNTING SYSTEM

1. Accounting information is stored and retrieved electronically using the Great Plains application, which is located on the internal CBT server at the Castlegar main office.
2. These records contain home addresses of committee members and individuals who have received reimbursements from CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (accounting activities).
4. The personal information is compiled and used for administering accounts payable and accounts receivable activities.
5. Finance staff, supervisors.

EMPLOYEE FILES

1. Employee files are located in the Human Resources Department and in the Semi-Active Records Storage room.
2. These files contain employment and benefit information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for employment-related purposes.

5. Human Resources staff, supervisors, employees.

IMS (INFORMATION MANAGEMENT SYSTEM)

1. Contract information and awards and bursary recipient information is stored and retrieved electronically using IMS application, which is located on the internal CBT server at the Castlegar main office.
2. These records contain home addresses of individuals with whom CBT has contracted, as well as home addresses of individuals who have received CBT scholarships and bursaries.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (financial administration activities).
4. The personal information is compiled and used for financial administration purposes.
5. Supervisors, employees.

PAYROLL FILES

1. Employee payroll files are located in the Finance Department and in the Semi-Active Records Storage room.
2. These files contain payroll information of current and former employees of CBT.
3. Section 26(a) of the *Freedom of Information and Protection of Privacy Act* (Income Tax Act); Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (employment program).
4. The personal information is compiled and used for employment-related purposes.
5. Finance staff, Human Resources staff, supervisors, employees.

PHOTO/VIDEO/AUDIO CONSENT FORMS

1. Signed consent forms are located in the Semi-Active Records Storage room and on the CBT server in Castlegar.
2. These records contain the name and signature of individuals who attend a CBT event and consent to their image/voice to be used for CBT marketing purposes.

3. Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (marketing activities).
4. The personal information is compiled and used for marketing purposes.
5. Communications staff.

RECORDS DATABASE

1. Descriptive information of physical CBT semi-active files are stored and retrieved electronically using the Records Database, which is located on the internal CBT server at the Castlegar main office.
2. The database contains titles of active and semi-active hard copy files, including the names of individuals with whom CBT has contracted and current and former employees.
3. Section 26(c) of the *Freedom of Information and Protection of Privacy Act* (recordkeeping activities).
4. The personal information is compiled and used for recordkeeping purposes.
5. Administrative staff, supervisors.

9. ADDITIONAL RESOURCES

Freedom of Information and Protection of Privacy Act

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

Office of the Information and Privacy Commissioner for British Columbia

<http://www.oipc.bc.ca/>

Ministry of Technology, Innovation and Citizens' Services

Freedom of Information and Protection of Privacy: Policy and Procedures Manual

http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page

Ministry of Technology, Innovation and Citizens' Services

Legislation, Privacy and Policy Branch

http://www.cio.gov.bc.ca/cio/priv_leg/lpp.page?

Ministry of Community Services

Freedom of Information and Protection of Privacy: Questions and Answers – Local Government Bodies (Updated September 2005)

<http://www.mser.gov.bc.ca/privacyaccess/main/LocalGovtQA.pdf>

Local Government Management Association of BC

Freedom of Information and Protection of Privacy Act Toolkit for Local Government Organizations (November 2012)

Available for purchase at <http://www.lgma.ca/>

APPENDIX A – TABLE OF ROUTINELY AVAILABLE RECORDS

The table below identifies common record types at CBT that are routinely available to the public. Should you receive requests for records that are not listed below, please contact the Manager, Business Systems.

SUBJECT HEADING
A
Acts and Legislation – General Information
Advertising – Articles, Postings, etc.
Agendas – Open Meetings (Board of Directors and Advisory/Board Committees)
Annual Reports
Application Forms – Blank
Application Forms – Completed
Appointments (Board of Directors and Board Committees)
B
BASINLink Newsletter
Board Committees – Open Meetings
Board of Directors – Appointments
Board of Directors – General Information
Board of Directors – Open Meetings (Agendas/Minutes)
Budgets – Annual Financial Report
Budgets – Operating – Final
C
Calendar of Events
Classifications – Jobs
Committees – Board – Agendas/Minutes – Open Meetings

SUBJECT HEADING
Corporate Governance – General Information
D
Delivery of Benefits Programs and Activities – General Information
E
Employee Classification
Environmental Programs – General Information
F
Financial Statements – Annual
Fire Inspection Reports (Buildings and Facilities)
Forms (various) – Blank
Funded Projects (List)
Funding and Program Information
G
Governance – General Information
Grants from CBT – General Information
H
I
Initiatives – General Information
Investments – General Information
J
Job Classifications
Job Descriptions
K
L
M
Media Releases
Minutes – Board of Directors and Various Committees – Open Meetings
Mission Statement
N
News Releases
Newsletters
Nominations – Board of Directors (appointed)
Nominations – Committees (appointed)
O
Operating Budgets – Final
Organizational Charts
P

SUBJECT HEADING
Policy and Procedures – Approved
Program Guides
Property Taxes Paid
Provisional Budget – Final
Publications
Q
Quotations – General Information
R
Reclassifications
Registration Forms – Completed
Remuneration – Board of Directors
Remuneration – Staff earning over \$75,000 per year
Report to Residents
Reports – Annual
Reports – Financial
Reports to Board of Directors – Open Meetings
Requests for Proposals/Quotations – General Information
Resolutions – Open Meetings
S
Salary Ranges – Job Descriptions
Signing Authorities (List)
Social Media Sites (i.e. Facebook, Twitter)
Speeches
Staff Reports – Open Meetings
Statistics
T
Tax Exemptions
Taxation Assessments
Taxes Paid
Tenders
Training and Development – General Information
U
V
W
Workshops – General Information
X, Y, Z
Youth Committee Members (List)

APPENDIX B – IDENTIFYING OFFICIAL AND TRANSITORY RECORDS

Each CBT employee must distinguish official business records from transitory records on a regular basis.

Transitory records are records in any form (paper, electronic, etc.) which are of short-term value and have no continuing administrative, operational, evidential, informational or archival value to the organization. Transitory records are defined as:

Records of temporary usefulness that are not an integral part of an administrative or operational records series, that are not regularly filed with a standard classification system, and that are only required for a limited period of time for the completion of an action or the preparation of an ongoing record. Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions.

Official records are records in any form which have been created, received and set aside during the regular conduct of business. Unlike transitory records, official records are of long-term value to CBT and have continuing administrative, operational, evidential, informational or archival value to the organization. All official records are to be maintained according to the corporate records management practices.

As a general rule, transitory records should be destroyed in an appropriate manner (i.e. shredded, recycled, deleted) once their usefulness has expired. The retention is “event driven” and not a fixed period of time; it may be as short as a few hours or as long as several days, weeks or months. Please note that some transitory records may be relevant to your work and should therefore be retained. See *Deciding Which Records Are Transitory* below for more information.

Examples of Transitory Records

Transitory records include, but are not limited, to the following examples:

- **Draft Documents and Working Materials**
Includes rough notes, research notes, and calculations used for the preparation of correspondence, reports, memoranda or other business records. May be disposed of once the final version of a document is complete and the master (original) filed.
 - **Note:** Not all drafts are transitory. In some cases, offices responsible for drafting legislation, legal documents, policy, budgets, standards, guidelines or procedures might need to track the evolution of the final product. These offices may need to keep various drafts, research and working materials in order to have a records of changes made and why.
- **Convenience or Reference Copies**
Records provided to you “for your information” (i.e. “cc” copies), which contain information that may be useful only for a brief period of time. Examples include:



- Routine notices or memos regarding holidays or special events circulated to all staff.
 - Print outs from databases, applications and the internet.
 - Issues that do not require your action.
- **Duplicate Copies**
Refers to exact copies of a record (photocopy, electronic copy, etc.) that have been created and retained only for the convenience of reference. Includes stocks of blank forms, internal information material, pamphlets, publications, etc., that have no further use to the organization.
- **E-mail**
Some e-mails are transitory records, whereas other are business records. If the e-mail meets the definition of a transitory record, then it can be deleted when no longer required. Otherwise, it is an official business record and must be managed accordingly.
- **External Publications**
Includes books, magazines, catalogues, directories, periodicals, pamphlets, brochures, journals, newspapers, and software documentation, whether printed or in electronic form, that are obtained from sources outside of the organization.
- **Outdated Lists**
Includes outdated address lists, distribution lists, membership lists, etc.
- **Transmission Documents**
Includes letters, fax cover sheets, e-mail message, routing slips, etc., that accompany documents but do not add value.

Deciding Which Records are Transitory

Determining whether a record is transitory depends on individual judgment of the value of the record. One employee could deem a record to be transitory while another considered it to be official, because the roles of the employees and their use of the information are different.

The key consideration is that if a record has only immediate or very short-term value to CBT and will not be required again after it is obsolete, you can dispose of it as soon as you are finished with it. But if the information in the record will have some future business, financial, legal, research or archival value to the organization, then you should retain and file it. If you are in doubt, keep the record.

Use the diagram below to help you identify records that are considered transitory and can be routinely destroyed (shredded, recycled, or deleted) as required.



Does the record (paper or electronic) provide evidence of a business activity, decision or transaction?

If No:

It is a Transitory Record and can be disposed of appropriately (deleted, recycled, or shredded)

If Yes:

Does it contain information that is only of immediate or short-term value?

Is it a duplicate copy?

Is it a draft that won't be of any value once the final document has been produced?

If Yes:

It is a Transitory Record and can be disposed of appropriately (deleted, recycled, or shredded).

If No:

Does it have future business, financial, legal, informational or archival value to CBT?

Does it provide evidence of compliance with accountability or other business requirements?

Is it needed to support business activities?

If Yes:

It is an **Official Record** and must be filed.



Comparison of Official and Transitory Records

Refer to this table for a quick reference to see if your records are official or transitory.

Official Records Maintain according to the Records Management Program	Transitory Records Destroy when no longer needed
<ul style="list-style-type: none"> • Advice, recommendations, and decisions, as well as background material • Policies, procedures, protocols, etc., as well as background material • Planning and budget records, as well as background material • Important telephone, e-mail, and face-to-face discussions • Contracts and other legal agreements, as well as background material • Proposed legislation and regulations, as well as background material • Proposed legislation and regulations, as well as background material • Work completed by consultants and others for the organization • All financial transactions • All records showing that services have been provided, or obligations have been incurred • All records that show that the organization's information systems have been maintained and are reliable 	<ul style="list-style-type: none"> • Temporary information, such as simple message, routing slips, and post-it notes • Duplicate copies of an official record that does not have comments written on it • Notes and rough drafts of letters, memos, reports, minutes, etc. <p>Note: If the information contains major revisions or helps to show how the final document was created, the record should be retained</p> <ul style="list-style-type: none"> • Publications from external sources, such as supply catalogues, brochures, magazines, etc. • Junk mail • Mass distribution notices, messages, and memos that do not directly affect your duties. If you send out the message, you should file it. • Outdated mailing lists, contact information, etc. • Unused forms, outdated business cards, brochures, etc.



Tips for Controlling Transitory Records

Here are some helpful tips for dealing with transitory records:

- Don't create unnecessary transitory records by downloading documents and distributing them as attachments. If possible, provide a link to the original web site instead.
- Discard duplicate print and electronic documents when you are sure the master (original) has been filed.
- Dispose of draft versions of documents and working materials that you don't need to keep when you are sure the final version has been distributed and the original filed.
- Securely destroy supplies of blank forms, letterhead/memo paper and business cards once they are obsolete.
- Discard routine, external publications once they have been circulated and/or you no longer need them, or once they are obsolete.
- Dispose of information with short-term value once you have acted on it.
- Dispose of advertising material and unsolicited mail as soon as you're finished with it.
- Review your e-mail messages regularly and delete transitory messages once they are obsolete.
- Erase voice mail messages after you listen to them; erase archived messages once you no longer need to save them.
- Shred transitory records containing confidential or sensitive information.

Key Points to Remember:

- A record that documents the evolution of a business decision or action is an official record, not a transitory record, and must be kept on file.
- Whether a record is transitory will depend on an individual's work requirements.
- Shred transitory records containing confidential or sensitive information.
- If in doubt, keep the record.



ARE YOU REQUESTING ACCESS TO ANOTHER PERSON'S PERSONAL INFORMATION? ☐YES ☐NO

IF YES, ATTACH EITHER: A) THAT PERSON'S SIGNED CONSENT FOR DISCLOSURE, OR
B)PROOF OF AUTHORITY TO ACT ON THAT PERSON'S BEHALF

PREFERRED METHOD OF
ACCESS TO RECORDS:

- ☐ EXAMINE ORIGINAL
- ☐ RECEIVE COPY – MAIL
- ☐ RECEIVE COPY – WILL PICK UP

YOUR SIGNATURE

DATE SIGNED
(DD/MM/YYYY)

PERSONAL INFORMATION CONTAINED ON THIS FORM IS COLLECTED UNDER SECTION 26(C) OF THE FREEDOM OF INFORMATION PROTECTION OF PRIVACY ACT AND WILL BE USED ONLY FOR THE PURPOSE OF RESPONDING TO YOUR REQUEST. FOR ASSISTANCE, CONTACT THE FOI COORDINATOR AT 250.304.1628.

APPENDIX D – PRIVACY IMPACT ASSESSMENT TEMPLATE

Please contact the Trust's Privacy Officer for the most recent version of the Privacy Impact assessment template.

APPENDIX E PROTECTING SENSITIVE INFORMATION OUTSIDE THE OFFICE

INTRODUCTION

To protect sensitive information, Trust employees must adhere to the following procedure when working in the field, from home or while travelling to protect paper and electronic records.

POLICIES

1. If you must take sensitive information with you, take only what you need and leave the rest behind. If possible, take copies and leave originals in the office.
2. Password-protect your electronic devices, plus any sensitive information you store on these devices. Use encryption, locks and alarms as appropriate.
3. Log off or shut down a device when not in use.
4. While away, keep devices and sensitive records with you at all times. For example, do not leave them in an unlocked office or meeting room, including during meals and other breaks.
5. If you must leave devices or records, place them in a secure location like a locked room or desk drawer. Consider storing them overnight at a local Trust office or in a hotel safe.
6. Only leave devices and records in a vehicle if there is no other option, and only if the vehicle is parked in a secure location for a brief period. Lock them in the trunk, not in plain view.
7. If working at home, store sensitive information in a locked filing cabinet or desk drawer that no one else can access. Avoid storing sensitive information on your home computer unless the information is encrypted and password-protected and the computer has security measures like anti-virus software and firewalls.
8. Avoid viewing or discussing sensitive information in public or while travelling. If you must do so, ensure no one can view or overhear the information.
9. Do not share work-designated devices with family members, friends and others.
10. Fax or photocopy sensitive information yourself, or have someone else do it only while you are present.
11. When you return to the office, return records to their original storage places as soon as possible and destroy the copies securely. Also store any sensitive notes you created in secure locations.
12. If sensitive information is stolen or lost, immediately notify your supervisor. If it is someone else's personal information that has been stolen or lost, immediately notify the Trust's privacy officer, and consider notifying the person affected and informing him or her that steps that are being taken to recover the information.

COLUMBIA BASIN TRUST FINANCE AND OPERATIONS POLICIES

Records Management

FOP24

INTRODUCTION

The purpose of this policy is to govern the classification, retention, maintenance and disposition of the Trust's records in support of the Records Management Program (RMP).

OBJECTIVE

The objectives of this policy are to:

1. Preserve the history of the Trust's activities;
2. Ensure that Trust records are complete and accurate;
3. Ensure records are available to support the Trust's informed decision-making;
4. Ensure the proper disposition of Trust records according to RMP policy, and maintaining auditable documentation;
5. Ensure the cessation of records destruction in the event of a litigation hold, audit process or FOIPPA request;
6. Protect sensitive and personal information from unauthorized access and disclosure;
7. Support accountable, efficient and economical business practices by reducing costs associated with creating, storing, and accessing records;
8. Meet legislative and regulatory requirements; and
9. Reduce exposure to risk and potential litigation.

POLICY

1. The Trust is committed to a RMP that is compliant with legislation, promotes accountability and transparency to the public, and meets access to information needs.
2. The RMP will ensure that records are retained as long as required for business, legal, audit, and informational purposes. A records classification system and retention schedule (RMP Procedures Manual) identifies all categories of Trust records and the corresponding retention requirements.
3. Any changes to the RMP or any associated document or procedure must be approved by either the Director, Finance and Operations or the President & CEO.
4. This policy applies to all records created, received, and/or maintained by Trust employees and those acting as agents in the course of their duties on behalf of the Trust (i.e. delivery partners or contractors), regardless of physical form or characteristic.
5. All records that are created by Trust employees, and by those acting as agents in the course of their duties on behalf of the Trust, are considered the property of the Trust and are subject to Trust control.

COLUMBIA BASIN TRUST

FINANCE AND OPERATIONS POLICIES

Records Management

FOP24

6. The roles and responsibilities associated with the Trust's RMP is as follows:
 - a) The President & CEO provides formal authority and support for the RMP and the retention and destruction of Trust records according to the Records Manual.
 - b) Information Services department provides overall direction and leadership for the RMP, including the development, implementation and monitoring of all RMP components and requirements for the Trust.
 - c) Information Services has the overall responsibility of coordinating the use and maintenance of technology across the Trust, including networks, databases, and stand-alone applications, such as the Information Management System (IMS).
 - d) All Trust employees are responsible for managing recorded information in accordance with the RMP.
7. Various provincial and federal legislation pertains to the Trust's recordkeeping and privacy protection responsibilities, including but not limited to the *Columbia Basin Trust Act* and the *BC Freedom of Information and Protection of Privacy Act* (FOIPPA).
8. Refer to the Intranet for access to current Records Management policies and forms.



RECORDS MANAGEMENT PROGRAM (RMP)

Procedures Manual

May 2020

TABLE OF CONTENTS

1. Introduction	3
2. Records Management Program (RMP) Overview.....	3
2.1. Introduction to Records Management	3
2.2. Records Defined	3
2.3. Recordkeeping Systems	3
2.4. Active Records in the Office.....	4
2.5. Naming Conventions	4
2.6. Official versus Transitory Records	6
2.7. File Maintenance Tips.....	6
3. Managing Inactive or Closed Records.....	7
3.1. Closing Files	7
3.2. Records Disposition.....	7
3.3. Preparation Procedures.....	7
3.4. Managing Permanent Records	8
3.5. Records Destruction	8
3.6. Records Destruction Processes.....	8
Appendix F: Forms	9
CLOSED BOX REPORT EXAMPLE	10
RECORDS DESTRUCTION AUTHORIZATION FORM	11

1. Introduction

The purpose of this manual is to provide Columbia Basin Trust (the Trust) employees with comprehensive guidance for creating and maintaining records in both paper and electronic formats according to the Records Management Program (RMP).

Questions regarding the Records Management Program may be directed to:

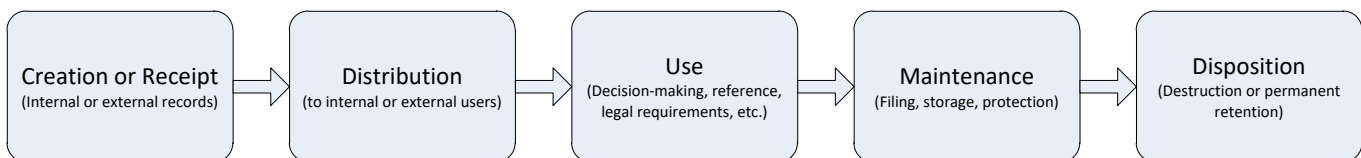
Dwayne Lau
Senior Manager, Information Services
Phone: 250.304.1670
E-mail: dlau@ourtrust.org

Lauren Quin
Records and Information Management Coordinator
Phone: 250.304.1669
E-mail: lquin@ourtrust.org

2. Records Management Program (RMP) Overview

2.1. Introduction to Records Management

Records Management can be defined as the systematic control of the creation, use, maintenance, storage, retrieval, and disposition of all forms of recorded information produced by an organization in the conduct of its operations.



2.2. Records Defined

Records are created (made or received) and set aside by a person or a corporate body in the course of practical activity. Records consist of all recorded information, and can exist in any format, i.e. paper, electronic, microfilm, photographic, audio-visual, etc.

Records are by-products of conducting business and are essential for the continuation of business. However, not all records are essential to retain over time. Records must have fiscal, legal, administrative, evidential and/or informational value to be maintained and preserved as evidence of functions, policies, decisions, procedures and operations.

2.3. Recordkeeping Systems

Records are maintained in one or more of the following types of office recordkeeping systems:

1. **LAN (Local Area Network), Shared Drives, and SharePoint Sites:** These can be organized and administered in accordance with RMP.

Storing records in employee-specific network drives or email folders is not equivalent to filing them in the office recordkeeping or shared filing system. Such storage may result in:

- 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 under FOIPPA or during the legal document discovery process

2. **Hardcopy paper files.** If required for business reasons paper records may be kept. Hard copy records may be digitized at any time in the future for convenience.

2.4. Active Records in the Office

Active records are those records held in filing cabinets within work areas, and are referenced frequently. Active records are typically not more than two years old, although records may remain active for more than two years. Records custodians have the ongoing responsibility to purge files-continually by reviewing folders and eliminating unnecessary paper, duplicates, and transitory documents. Staff are responsible for annually reviewing office file cabinets to remove the following categories of files:

1. Scheduled for immediate destruction.
2. Semi-active storage required (in a designated semi-active records storage centre).

2.5. Naming Conventions

In order to facilitate information retrieval, it is important to use standard naming conventions for all physical (hard copy) and electronic records.

Naming Electronic Folders and Documents

Electronic and physical folders bring together a set of records about the same activity, topic or transaction. The title must clearly identify this purpose.

When creating an electronic folder or document name, employees should:

- Create unique, concise, meaningful titles that will facilitate retrieval;
- Ensure the title contains enough information for anyone else to identify it; and
- Order the elements in a document name in the most appropriate way to retrieve the records.
- Avoid using common words such as 'draft' or 'letter' in the document names, as this can result in documents being grouped together when they shouldn't be.
- Avoid using abbreviations and acronyms in a folder or document name unless it is commonly understood and used by everyone in the organization, and will likely have the same meaning 5 to 10 years in the future.
- Avoid using spaces, symbols and characters (\$, #, ., <, &, " etc.) in electronic folder/file names, as they can impair current and future search capabilities.
- Use capital letters to delimit words. () Underscores or (-) dashes may be used if necessary.
- Consider using file name and file path in the footer of a document, especially for documents that are likely to be accessed by several employees.
- When naming electronic documents, employees should follow this naming convention:
DocumentTitleDocumentDateVersionNumberStatus.file extension
 - Correct: NamingGuidelines2015-07-21v1draft.docx
 - Incorrect: Draft Naming Guidelines July 21 2015 draft 1.docx

Optional Elements

- **Document Date** – use the International Date Standard YYYY-MM-DD to indicate the date a document is created. This method will permit electronic documents to sort in the correct date order.
 - **NOTE:** 2015Jul21 format is also currently acceptable.
- **Version Number** – use a one digit version number to distinguish one version from subsequent revisions. Should more than 10 versions be anticipated, use two digit version numbers.
- **Status** – indicates the status of the document, such as draft or final.
- **Initials** – staff initials may be included to indicate who contributed comment to collaborative document.

Naming Physical File Folders

Folders or files bring together a set of records about the same activity, topic or transaction. In cases where hard copy records are housed in binders, the binder is considered the equivalent of a folder and should be named using the same standard.

General Rules

- A title should act as a summary of the file or record's contents and purpose. Make the name of a file or record descriptive of the whole content while being brief and concise.
- Ensure the title contains enough information for anyone else to identify it.
- Balance being concise with being descriptive.
- Avoid using the name of a person in the title of a folder, file, document or record for privacy purposes. If you must refer to someone, use their job title rather than their name.
- Avoid using common words such as 'old' or 'new' in the title of a folder or document. It is best to use the words "pre-" and "post-" a specific date or event where a range of document dates apply.
- Avoid using abbreviations and acronyms in a folder or document name unless it is commonly understood and used by everyone in the organization, and will likely have the same meaning 5 to 10 years into the future.

Required Elements

Every physical file folder (or binder) title should include the following elements (or components):

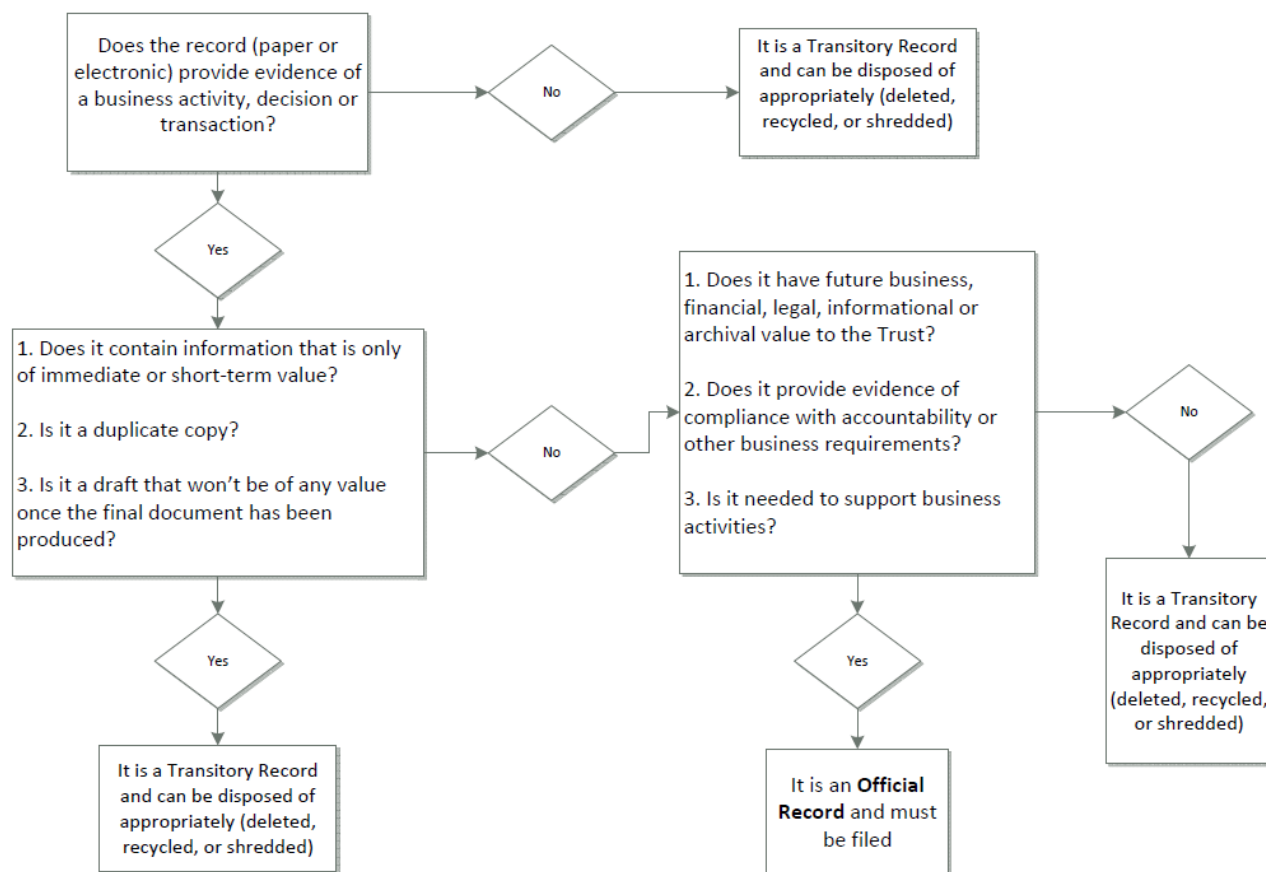
- **File Classification Number** – the 8 digit code that represents the appropriate classification of the Records Manual
 - Example: 03-7000-40
- **File Title** – should reflect the business procedure, project, program or initiative to which the folder contents relate. Only use abbreviations or acronyms if they are commonly used and understood.
- **Inclusive Dates** – the date range that applies to the contents of the folder. This may be a specific date, a calendar year, or a span of calendar/fiscal years
 - Example: 2014, 2014-2019

Optional Elements (use if applicable)

- **File Identifier** – represents a unique project or case file.
 - Example: IMS#1234
- **Volume Number** – if the folder is one component of a larger file that includes multiple folders, use a Volume Number to show how that particular folder fits into the larger file.
 - Example: "Environment Strategic Plan – Vol. 1, Environment Strategic Plan – Vol. 2" or "Environment Strategic Plan – Correspondence", Environment Strategic Plan –Background Material"

2.6. Official versus Transitory Records

Determining whether a record is transitory depends on individual judgement of the value of the record. One employee could deem a record to be transitory while another considered it to be official, because the roles of the employees and their use of the information are different. Use the diagram below to help you identify records that are considered transitory and can be routinely destroyed (shredded, recycled, or deleted) as required.



2.7. File Maintenance Tips

Electronic Files

1. Save all official electronic records in the N:/ drive (TrustDrv).
2. Upload all contract and project-related records to the CRM system. Copies may be saved to the N:/ drive for convenience.
3. Utilize naming conventions.
4. Limit the number of subfolders you create wherever possible. This reduces the number of “clicks” to access the information at a later time.
5. Regularly review folder contents and delete any transitory records, three to four times per year, if possible.
6. Schedule time in your calendar for records management. Start with an hour once a week.

Physical Files

1. Review file for completeness.
 - “Are all attachments and enclosures actually attached?”

- May involve a combination of hard copy and electronic records
- 2. Remove all transitory records.
- 3. Remove paper clips, rubber bands, and extra staples.
- 4. Retain photocopies of newspaper clippings rather than newspaper because of the high level of acidity in the paper.
- 5. Ensure the date and name of newspaper articles is legibly marked on the copy.
- 6. Fold maps and oversized documents so that they can be viewed without removing them from the file.
- 7. Do not file electronic media in physical files.
 - Maintain a separate CD/DVD collection within your department (store disks in sleeves and stand on edge)
- 8. Create a new volume or open a new file when file thickness exceeds 1 inch.
- 9. Mark files as “closed” when appropriate.
- 10. Write any helpful cross-reference notes on the inside of the file folder to enable users to access all related records.

3. Managing Inactive or Closed Records

When records are no longer referenced for daily work, they are deemed to be “closed”, “semi-active” or “inactive.” When this occurs, the files may be removed to storage. The rationale for removing them is to free up space, and ensure the ongoing accessibility for those records still active.

3.1. Closing Files

Records are closed at a logical time, typically at year end or when a project is complete. For several types of files, an event-based conditional retention trigger is required, such as “retain until employment ceases.” In this case, the inactive state begins when the condition of employment is completed. When records are closed, the folder must be closed electronically or in a paper format.

3.2. Records Disposition

The last phase in the record life cycle is *disposition*, which is to either destroy records or to transfer records to a dedicated storage area for continued preservation. Along with legislative retention requirements, departmental needs are taken into consideration in determining the final disposition of records which have reached the end of their life cycle.

3.3. Preparation Procedures

Preparing Electronic Records for Archival Storage

To store electronic records that will allow for future viewing the records must be converted to a PDF-A file and moved to the Archive folder.

Step 1: Ensure folder name and document naming conventions have been applied.

Step 2: Convert documents to a PDF-A Format.

Step 3: Copy and Paste the folder to the Archive drive

Step 4: Delete records from original location

Preparing Paper Records for Storage

Wherever boxes of files are being stored, the contents of each box must be identified. The following steps will guide you through the process of preparing and moving your records to a designated storage area.

Step 1: All records should be in letter size folders. Each folder should have the folder name and the classification code written on the folder tab or printed on a file label.

Step 2: Review and remove all records that do not comprise a permanent part of the file. These include documents such as duplicate copies, convenience copies, fax cover sheets, draft versions of completed agreements, etc. (See the “Official vs. Transitory Records” above for more information.)

Step 3: Pack records into an appropriate records storage boxes, often called “Bankers Boxes”. Boxes should be full, but not overstuffed. Hanging folders must not be used in storage boxes.

Step 4: Create a Box Inventory List (see Appendix A) for each box to be stored and attach such list to the two short sides of the box.

3.4. Managing Permanent Records

Business records having permanent value to the Trust are identified through the RMP. Permanent records are preserved as evidence of functions, policies, decisions, procedures and operations of the organization, as well as material of historical significance to residents and communities of the Columbia Basin. Permanent Records that are being stored digitally must be archived to the identified network location using the preferred format of PDF-A 1b or 2b.

Retrieving Files from Storage

From time to time staff may need to access records that are kept in the records storage area. For various reasons, it is important to keep track of when files in storage are accessed, and by whom. To request files from off-site storage, contact the Administrative Assistant, Records via email.

3.5. Records Destruction

The final stage in the life cycle of information is the disposal of records. Records disposal occurs when there are no longer requirements for the information. Once the Trust has an approved retention schedule, the planned disposal of records is part of the “usual and ordinary course of business” of how the organization makes and keeps records. Formal approval of the Trust’s Records Retention Schedule provides the organization with an approved and controlled method of destroying official records.

3.6. Records Destruction Processes

Step 1: Use the Records Management Database to identify those files that are in offices, in storage areas or on the network drive, that are scheduled for destruction in the current year according to their Records Manual classification (DE for destruction).

Step 2: Gather those files into a single physical or electronic location. Files may be collected from multiple offices or folders and put into a box or location marked “Destroy December 2015”.

Step 4: Fill out a Destruction of Records Authorization Form (see Appendix A). If you have a number of files falling under the same classification you can group them together rather than listing each individual file. If you are requesting destruction of an entire box from storage, enter the box information on the request form and attach a copy of the Box Inventory List to the form.

Step 5: Once the Authorization for Destruction of Records form is complete, it must be signed by the Director or Manager responsible for the records, Senior Manager, Information Services and Chief Executive Officer.

Step 6: Physical records must brought to the appropriate location for shredding. Delete associated electronic records from the network drive. Keep a copy of the signed Authorization form for your records and provide one copy to the Administrative Assistant, Records.

Appendix F: Forms

Includes:

1. Closed Box Report - Example
2. Authorization for the Destruction of Records

CLOSED BOX REPORT EXAMPLE

Box
Number

File

File Title

From

To

A

SA FD

001

02-5000-30 -	YSCA Declined Applications			EV+1	nil	DE
02-5000-30 -	YCSA Successful Applications			EV+1	nil	DE
02-5000-40 - 10528	Art Workshops for Young Artists			EV+1	6y	SR
02-5000-40 - 10534	Kaslo/Castlegar Arts/Education Outreach			EV+1	6y	SR
02-5000-40 - 10535	Youth Impact Summer Program			EV+1	6y	SR
02-2000-40 - 10617	Pilot Special Needs Camp			EV+1	6y	SR
02-3000-40 - 10642	Aquatic Environmental Sciences Education Program			EV+1	6y	SR
02-3000-40 - 10646	Parks Interpretation East Kootenays			EV+1	6y	SR
02-3000-40 - 10648	Outdoor Experience Enhancement			EV+1	6y	SR
02-3000-40 - 10650	Kokanee Visitors Centre			EV+1	6y	SR
02-5000-40 - 10818	Games Club			EV+1	6y	SR
02-6000-50 - 10844	Abattoirs in the Basin			EV+1	6y	DE
02-5000-40 - 10900	Columbia Salmon, Past, Present, Future			EV+1	6y	SR
02-6000-50 - 10902	Keeping it Rural 2015 Conference			EV+1	6y	DE
02-5000-40 - 10910	NYC Summer Program			EV+1	6y	SR
02-5000-40 - 10914	Kids These Days			EV+1	6y	SR
02-5000-40 - 10919	Youth Polish Shine and Show Clinic			EV+1	6y	SR
02-6000-50 - 11225	Winlaw School Peace Day			EV+1	6y	DE

Originating Department/Office	Prepared by	Date
-------------------------------	-------------	------

RECORDS DESTRUCTION AUTHORIZATION FORM

1. Describe paper and electronic records in Part A and indicate location of records.
2. If the retention period needs to be extended for operational, legal, or other purposes, indicate the rationale in Part B.
3. Authorize destruction in Part 3 and forward to Administrative Assistant and Records.
4. Certify destruction activity in Part 4.

A RECORDS DESCRIPTION

Class. No.	Record Series / Folder Titles / Box Name (attach list as required)	Date Range (In years)	Originals Yes or No	Location	Destruction Method	Scheduled Destruction Date
Total No. Boxes						

B RETENTION EXTENSION

Explain any rationale to retain specific records for a longer period of time, such as litigation support, operations, etc.

Class. No. & Records Series (attach list) and Rationale	Box No.	Extended Destruction Date

C AUTHORIZATION TO DESTROY

Manager/Director (name and signature)	Date
Administrative Assistant and Records (name and signature)	Date
Chief Executive Officer (name and signature)	Date

D CERTIFICATE OF DESTRUCTION

Administrative Assistant and Records (name and signature)	Destruction Method	Date
---	--------------------	------



BC Freedom of Information and Protection of Privacy Act (FOIPPA/FIPPA)

May 2021

Columbia
Basin **trust**



Agenda/House Keeping

- Privacy Contacts
- The Act
- Protecting Privacy
- Records Management
- Information requests
- Privacy Impact Assessments
- Collection notices
- Available Resources and Questions

Privacy Contacts

- Head of the public body – Board Chair -> delegated to CEO
- FOI Manager/Privacy Officer (Dwayne)
- FOI Coordinator (Lauren)
- Office of the Information Privacy Commissioner (OIPC)
- All Staff:
 - Understand FOIPPA and our obligations
 - Understand and apply records management practices and adhere to policies
 - Release routinely releasable information
 - Forward information or record requests to FOI Coordinator

The Act

FOIPPA was introduced in 1994 and applies to all public bodies within the Province

- Makes public bodies more accountable by providing the public with a legislated right of access to records, and
- To protect personal privacy

	Public sector	Private sector
Federal	<ul style="list-style-type: none">• Access to Information Act• Privacy Act	<ul style="list-style-type: none">• Personal Information Protection and Electronic Documents Act (PIPEDA)
BC	<ul style="list-style-type: none">• Freedom of Information and Protection of Privacy Act (FOIPPA)	<ul style="list-style-type: none">• Personal Information Protection Act (PIPA)

The Act cont...

- Scope: applies to all records in the **custody or under the control** of a public body

Custody: (out of OIPC Order)

physical possession of records is not enough to establish custody and that a public body will only have custody if it has “some right to deal with the records and some responsibility for their care and protection.

Control:

Have the right to access the record and control its disposition.

- Duty to assist *“must make every reasonable effort to assist applicants and respond without delay”*

Protecting Privacy

- Only collect personal information if it relates directly to and is necessary for an operating program or activity, or if the individual has consented to the prescribed purpose
- Use personal information for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose
- Protect, secure, store in Canada etc.
- You own your own personal information. You have the right to control it's collection, disclose, and use wherever it is held

Personal vs Contact Information

“Recorded information about an identifiable individual other than contact information” (PII)

VS

“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.”

Personally identifiable (PII)??

- Home address
- Work phone number
- Job responsibilities (public sector employee)
- An individuals opinion about an employee
- IP Address
- Dietary restrictions

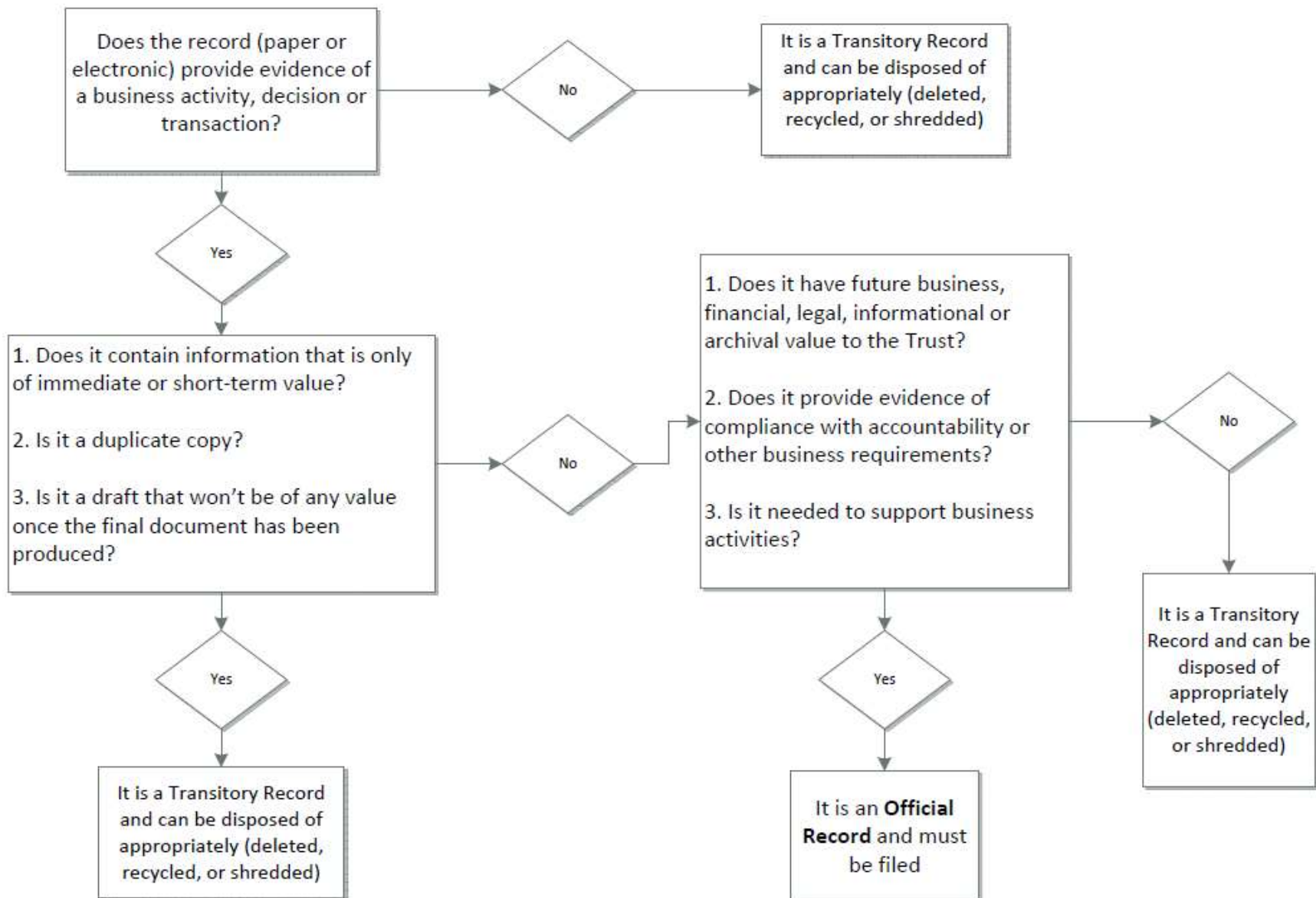
Records Management

FOIPPA defines records as “recorded information”:

“Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records”

Transitory vs Official Information

- Information is considered transitory when it does not document decisions or work activities
- Transitory information holds temporary usefulness that is needed only for a limited of time
- An official record is any record that is essential to understanding business and must be kept as per our records management practices



Transitory Record Examples

- Meeting arrangements
- Personal messages
- CC Copies
- Routine correspondence about drafts and revisions
- And more

Official Record Examples

- Work schedules
- Final reports
- Policies and directives
- Meeting agendas and minutes
- And more

SKILL TEST #1

- Is the following record transitory or official?

Tue 04/20/2021 10:50 AM

✓ Dwayne Lau

Accepted: FOIPPA Training Run Through #1

To ✓ Lauren Quin

When April 26, 2021 9:00 AM-10:30 AM (UTC-08:00) Pacific Time (US & Canada).

Location Microsoft Teams Meeting

Accepted No attendees have accepted.

Tentative No attendees have tentatively accepted.

Declined No attendees have declined.

i Dwayne Lau has accepted this meeting.

SKILL TEST #2

- Is the following record transitory or official?

CONTRIBUTION AGREEMENT

ROCKY MOUNTAIN TRENCH NATURAL RESOURCES SOCIETY

Box 151
Kimberley, BC V1A 2Y6

('Recipient')

WHEREAS in accordance with the Trust's purp
Trust wishes to provide a grant for the project d
the Recipient and the Recipient has the capacit

NOW THEREFORE this Agreement witnesses
contained, the parties agree as follows:

COLUMBIA BASIN TRUST

Suite 300, 445 – 13th Avenue
Castlegar, BC V1N 1G1

This Agreement has been executed on behalf of the Trust and the Recipient as of the dates indicated below:

Rocky Mountain Trench Natural Resources Society

Signed by:



Name: ~~Michael [Redacted]~~

Title: ~~Coordinator~~

Date: ~~January 18, 2021~~

Columbia Basin Trust

Signed by:



Name: Aimee Ambrosone

Title: Executive Director, Delivery of Benefits

Date: January 18, 2021

SKILL TEST #3

- Is the following conversation transitory or official?

The screenshot shows a Microsoft Teams chat window with the following content:

Lauren Quin 3/25 10:53 AM
Visitor Centre Wage Subsidy Program PIA
Sandra Haley, Will Nixon, Patrick Checknita
Sandra & Will - Please see comments added to your PIA and update sections as required. Please let me know when complete or if you have questions

Dwayne Lau 4/12 8:00 AM
I've reviewed the PIA and have some clarifying questions so I understand things a little better:
Will Nixon

- This program is delivered by Visitor Centres that we fund through CA's. Eg PProject 17640 - Castlegar
- Personal information (PII) is being collected as per PIA, using Schedule C form from the CA
- That PII is being stored by Visitor's Centre as well as being provided to the Trust - *Correct?*


[See more](#)

Will Nixon All poir

Lauren Quin 4/13 2:53 PM
Will Nixon, before we can approve for signing we need a bit more detail from yourself or your team on this PIA:

- Please add a privacy schedule (one can be pulled from an old program and attached), this will give us a better idea of the data flow.
- Please review and update/respond to comments added to the PIA

[See more](#)

Dwayne Lau 4/13 3:33 PM
Thanks Lauren, maybe just clarifying. As this program is more of a delivery partner relationship with another entity doing registrations and keeping records (like other student wage subsidy programs), we recommend considering including a Privacy and potentially a Confidentiality schedule to the Contribution Agreements. I believe this isn't part of the basic CA template but has been included in some other selected CA's. tks,  1

Classification System snippet

07-1000 Access and Privacy

Records related to the management of access to information and protection of privacy issues as stipulated in the *Freedom of Information and Protection of Privacy Act (FOIPPA)*. Includes reviews by the Office of the Information and Privacy Commissioner (OIPC) of the Trust's responses to requests for records as regulated by *FOIPPA*.

For the Trust's FOIPPA Procedures Manual, see 03-6000-40.

07-1000-30 Operations

07-1000-30

Privacy Impact Assessments Files

EV+1 nil DE

Records documenting the preparation of Privacy Impact Assessments (PIAs), in accordance with s. 69 of *FOIPPA*. Privacy Impact Assessments are conducted to determine if new programs, systems, or projects meet the requirements of part 3 of *FOIPPA*. Records may

include correspondence, reference material, working notes, completed PIAs, and other supporting documentation.

EV = Upon completion of a new PIA, or disposal of records covered by the PIA

OPR: Operations

Email Management

- Avoid “reply-all” or “hi-jacking” email subjects
- We do not redact for poor grammar or inappropriate comments
- Delete transitory records regularly

Information Requests

Anyone can make an information request

- Questions from the public
- Request for routinely available records
- Formal FOI request

When an information request moves to a formal FOI request, we are obligated to respond within 30 working business days

Routinely Releasable Examples

- Annual Reports
- Brochures and other publications
- Approved bylaws and resolutions
- Board of directors agendas and minutes
- Approved Budgets
- Maps
- Program Information (General)
- Statistical Information
- Any records published to public website

Formal FOI Process

Receive Request

- Any Trust staff, delivery partner, contractor, or consultant
- Request must be in writing
- Forward to FOI Coordinator
- 30 business days to respond

Process Request

- The FOI Coordinator collaborates with Head, departments and/or delivery partners
- Background investigation – email e-discovery – IMS search – Networks drives
- Third party notices
- Review and redact records

Response

- The FOI Coordinator Response package prepared and provided to the CEO (Trust) or Chair (CPC) for approval
- Ministry is advised of request
- Package released to applicant
- Applicant may request a review to OIPC within 30 days of receipt

PIA's (Privacy Impact Assessment)

- Required for new initiatives and programs through any of our departments
- Valuable tool to evaluate privacy impacts and ensure compliance on personal information

PIA Process

Teams Channel

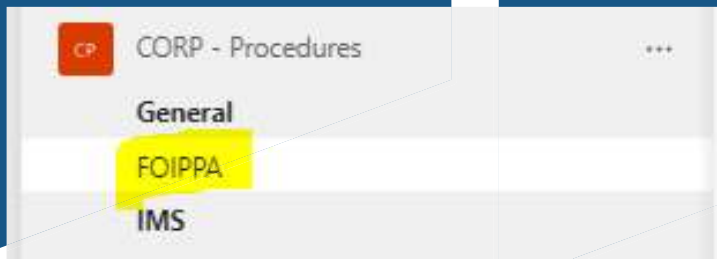
- Create new post with initiative name and launch date
- Tag FOI Coordinator

FOI Coordinator

- Creates PIA # and draft PIA
- Tags Business Unit to continue draft PIA

Business Unit/FOI Coordinator

- Business unit completes Part 1, tags FOI Coordinator when complete
- FOI Coordinator reviews for personal information
- If personal information is included, we complete remainder of PIA



Collection Notices

- Required under the Act when collecting personal information
- Public bodies must only collect personal information for the following purposes:
 - The information relates directly to and is necessary for an operating program or activity
 - With respect to a prescribed purpose, the individual has consented to their collection

Pre-Approved Collection Notice Language

By submitting this application I acknowledge the following:

The personal information requested in this application and subsequent submissions is collected under the authority of section 26(c) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA), and will be used by Columbia Basin Trust for administrative and evaluative purposes relating to the **(initiative/program)**. The collection, use and disclosure of personal information is subject to the provisions of the FOIPPA. Any questions regarding such may be directed to: FOIPPA Inquiries, Senior Manager, Information Services, Columbia Basin Trust, Suite 300, 445-13 Ave., Castlegar, BC V1N 1G1, 1-800-505-8998

Summary – Protecting Privacy

- Only collect what you need to collect
- Only use it for the purpose you collected it for
- PIA's are a valuable tool for assessing privacy impacts
- A collection notice is required when personal information is being collected

Summary – Records Management

- Release routinely releasable records when possible
- Report a formal FOI request immediately
- Follow records management practices/policies
- Delete transitory records/manage email

Resources

Records Mgmt and Privacy – Intranet

- [Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#)

Records Management Resources & FAQ's

- RMP – Intranet
- Classification System – Intranet
- Transitory Flowchart – Intranet

Privacy Resources & FAQ's

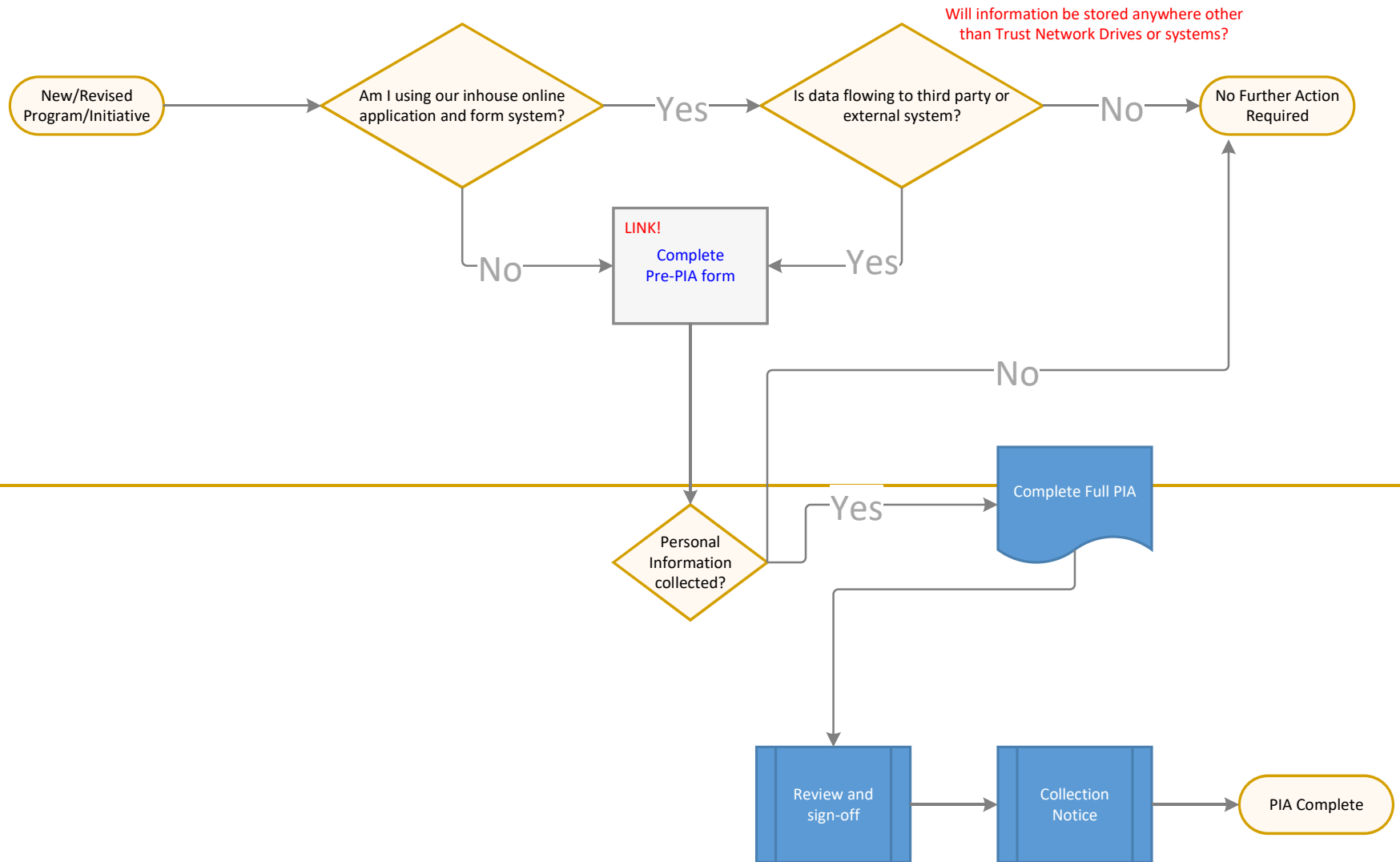
- Collection notice example – Intranet
- Quick reference guide – Intranet
- Draft PIA's – Teams Channel
- 2021 FOIPPA Training – Coming soon to the Intranet

Thank You
Questions?

PIA Flowchart

Business Unit

Privacy Department



PrivacyWorks.

PrivacyWorks Service Agreement

PrivacyWorks Consulting Inc.

4469 Percival Ave.,
Burnaby, British Columbia
V5G 3S4
(Hereinafter referred to as "PrivacyWorks")

And

Columbia Basin Trust
445 13Th Avenue
Castlegar, BC
V1N 1G1
Canada
(Hereinafter referred to as "the Company")

Services

Working under the direction of Adrian Chalifour, FOI/ATIP Manager, and Adam Stinson, CEO, PrivacyWorks will deliver FOI and Privacy consulting services to the Company as part of its service offering. The scope of these services will be discussed and determined in collaboration with the Company. The services may include but are not limited to the following:

- End-to-end FOI request processing support
- FOI advisory and coaching services
- FOI Training
- Developing Privacy Impact Assessments
- Privacy Training
- Other Ad hoc services as needed

Compensation

Subject to providing the services, the Company will pay PrivacyWorks \$150 CAD per hour plus GST for privacy related services and \$125 CAD per hour plus GST for Freedom of Information request related services.

Hours will be scoped on an as-needed basis. Any time worked in excess of 50 hrs/month will require approval from the Company in advance. PrivacyWorks will invoice the Company at the end of each month for hours worked. Invoices are payable within 30 days of receipt.

Term

The term of this Agreement shall begin on July 1, 2022 and continue until such time as services are no longer required or one (or both) parties conclude the arrangement. The term of this Agreement may be extended by mutual agreement between the parties.

Relationship

PrivacyWorks will provide the services to the Company as an independent contractor and not as an employee. Accordingly: PrivacyWorks agrees that the Company shall have no liability or responsibility for the withholding, collection or payment of any taxes, employment insurance premiums or Canada Pension Plan contributions on any amounts paid by the Company to PrivacyWorks or amounts paid by PrivacyWorks to its employees or contractors. PrivacyWorks also agrees to indemnify the Company from any and all claims in respect to the Company's failure to withhold and/or remit any taxes, employment insurance premiums or Canada Pension Plan contributions.

PrivacyWorks agrees that as an independent contractor, PrivacyWorks will not be qualified to participate in or to receive any employee benefits that the Company may extend to its employees. PrivacyWorks is free to provide services to other clients, so long as such other clients are not in competition with the Company and so long as there is no interference with PrivacyWorks' contractual obligations to the Company.

PrivacyWorks has no authority to and will not exercise or hold itself out as having any authority to enter into or conclude any contract or to undertake any commitment or obligation for, in the name of or on behalf of the Company.

Confidentiality and Intellectual Property

PrivacyWorks hereby acknowledges that it agrees to be bound by the terms and conditions of the confidentiality and proprietary information agreement attached hereto as Schedule "A" and which forms an integral part of this Agreement. If PrivacyWorks retains any employees or contractors of its own who will perform services hereunder, PrivacyWorks shall ensure that such employees or contractors execute an agreement no less protective of the Company's intellectual property and confidential information than the attached agreement.

PrivacyWorks hereby represents and warrants to the Company that it is not party to any written or oral agreement with any third party that would restrict its ability to enter into this Agreement or the Confidentiality and Proprietary Information Agreement or to perform PrivacyWorks' obligations hereunder and that PrivacyWorks will not, by providing services to the Company, breach any non-disclosure, proprietary rights, non-competition, non-solicitation or other covenant in favour of any third party.

PrivacyWorks hereby agrees that, during the term of this Agreement and for one (1) year following the termination hereof, PrivacyWorks will not (i) recruit, attempt to recruit or directly or indirectly participate in the recruitment of any Company employee or (ii) directly or indirectly solicit, attempt to solicit, canvass or interfere with any customer or supplier of the Company in a manner that conflicts with or interferes in the business of the Company as conducted with such customer or supplier.

Termination

This Agreement may be terminated by either party at any time and without further obligation or liability immediately upon written notice by either party for non-performance, default or breach of this Agreement by the other party.

Obligations Surviving Agreement

All obligations to preserve the Company's Confidential Information, Intellectual Property and other warranties and representations set forth herein shall survive the termination of this Agreement.

Entire Agreement

This Agreement, together with the Confidentiality and Proprietary Information Agreement, represents the entire agreement between the parties and the provisions of this Agreement shall supersede all prior oral and written commitments, contracts and understandings with respect to the subject matter of this Agreement. This Agreement may be amended only by mutual written agreement of the parties.

Assignment

This Agreement shall inure to the benefit of and shall be binding upon each party's successors and assigns. Neither party shall assign any right or obligation hereunder in whole or in part, without the prior written consent of the other party.

Governing Law

This Agreement shall be governed and construed in accordance with British Columbia law. If any provision in this Agreement is declared illegal or unenforceable, the provision will become void, leaving the remainder of this Agreement in full force and effect.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives, effective as of the day and year first above written.



Adam Stinson, CEO

08 / 03 / 2022



Dwayne Lau, Senior
Manager, Information
Services

08 / 04 / 2022

Schedule A

Confidentiality and Proprietary Information Agreement

In consideration of an engagement as an independent contractor or consultant with Columbia Basin Trust (the "Company"), the undersigned (the "Contractor") agrees and covenants as follows:

1. Engagement with the Company as an independent contractor or consultant ("Engagement") will give the Contractor access to proprietary and confidential information belonging to the Company, its customers, its suppliers and others (the proprietary and confidential information is collectively referred to in this Agreement as "Confidential Information"). Confidential Information includes but is not limited to customer lists, marketing plans, proposals, contracts, technical and/or financial information, databases, personal information, software and know-how. All Confidential Information remains the confidential and proprietary information of the Company.
2. As referred to herein, the "Business of the Company" shall relate to the business of the Company as the same is determined by the Board of Directors of the Company from time to time.
3. The Contractor may in the course of the Contractor's Engagement with the Company conceive, develop or contribute to material or information related to the Business of the Company, including, without limitation, software, technical documentation, ideas, inventions (whether or not patentable), hardware, know-how, marketing plans, designs, techniques, documentation and records, regardless of the form or media, if any, on which such is stored (referred to in this Agreement as "Proprietary Property"). The Company shall exclusively own, and the Contractor does hereby assign to the Company, all Proprietary Property which the Contractor conceives, develops or contributes to in the course of the Contractor's Engagement with the Company and all intellectual and industrial property and other rights of any kind in or relating to the Proprietary Property, including but not limited to all copyright, patent, trade secret and trade-mark rights in or relating to the Proprietary Property. Material or information conceived, developed or contributed to by the Contractor outside work hours on the Company's premises or through the use of the Company's property and/or assets shall also be Proprietary Property and be governed by this Agreement if such material or information relates to the Business of the Company. The Contractor shall keep full and accurate records accessible at all times to the Company relating to all Proprietary Property and shall promptly disclose and deliver to the Company all Proprietary Property.
4. The Contractor shall, both during and after the Contractor's Engagement with the Company, keep all Confidential Information and Proprietary Property confidential and shall not use any of it except for the purpose of carrying out authorized activities on behalf of the Company. The Contractor may, however, use or disclose Confidential Information which:
 - (I) is or becomes public other than through a breach of this Agreement;
 - (II) is known to the Contractor prior to the date of this Agreement and with respect to which the Contractor does not have any obligation of confidentiality; or
 - (III) is required to be disclosed by law, whether under an order of a court or government tribunal or other legal process, provided that Contractor informs the Company of such requirement in sufficient time to allow the Company to avoid such disclosure by the Contractor.
5. The Contractor shall return or destroy, as directed by the Company, Confidential Information, Proprietary Property and any other Company property to the Company upon request by the Company at any time. The Contractor shall certify, by way of affidavit or statutory declaration, that all such Confidential Information, Proprietary Property or Company property has been returned or destroyed, as applicable.

6. At the reasonable request and at the sole expense of the Company, the Contractor shall do all reasonable acts necessary and sign all reasonable documentation necessary in order to ensure the Company's ownership of the Proprietary Property, the Company property and all intellectual and industrial property rights and other rights in the same.

7. The Contractor hereby irrevocably and unconditionally waives all moral rights the Contractor may now or in the future have in any Proprietary Property.

8. The Contractor agrees that the Contractor will, if requested from time to time by the Company, execute such further reasonable agreements as to confidentiality and proprietary rights as the Company's customers or suppliers reasonably require to protect confidential information or proprietary property.



9. Regardless of any changes in position, fees or otherwise, including, without limitation, termination of the Contractor's Engagement with the Company, unless otherwise stipulated pursuant to the terms hereof, the Contractor will continue to be subject to each of the terms and conditions of this Agreement and any other(s) executed pursuant to the preceding paragraph.

10. This Agreement is governed by the laws of the Province of British Columbia and the parties agree to the non-exclusive jurisdiction of the courts of the Province of British Columbia in relation to this Agreement.

If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, that provision shall be deleted and the other provisions shall remain in effect.

Signature Certificate

Reference number: TXXJH-CXYCB-3RKRM-G2YGJ

Signer	Timestamp	Signature
Torin Regier Email: torin@privacyworks.ca Sent: 04 Aug 2022 08:39:07 UTC Viewed: 04 Aug 2022 08:39:20 UTC Signed: 04 Aug 2022 08:39:43 UTC		 IP address: 213.31.168.16 Location: Newtonmore, United Kingdom
Dwayne Lau Email: dlau@ourtrust.org Sent: 04 Aug 2022 08:39:07 UTC Viewed: 04 Aug 2022 15:54:25 UTC Signed: 04 Aug 2022 15:55:17 UTC		 IP address: 162.245.240.195 Location: Castlegar, Canada
Recipient Verification: ✓Email verified	04 Aug 2022 15:54:25 UTC	

Document completed by all parties on:
04 Aug 2022 15:55:17 UTC

Page 1 of 1



Signed with PandaDoc

PandaDoc is a document workflow and certified eSignature solution trusted by 30,000+ companies worldwide.



FOIPPA Quick Reference Guide

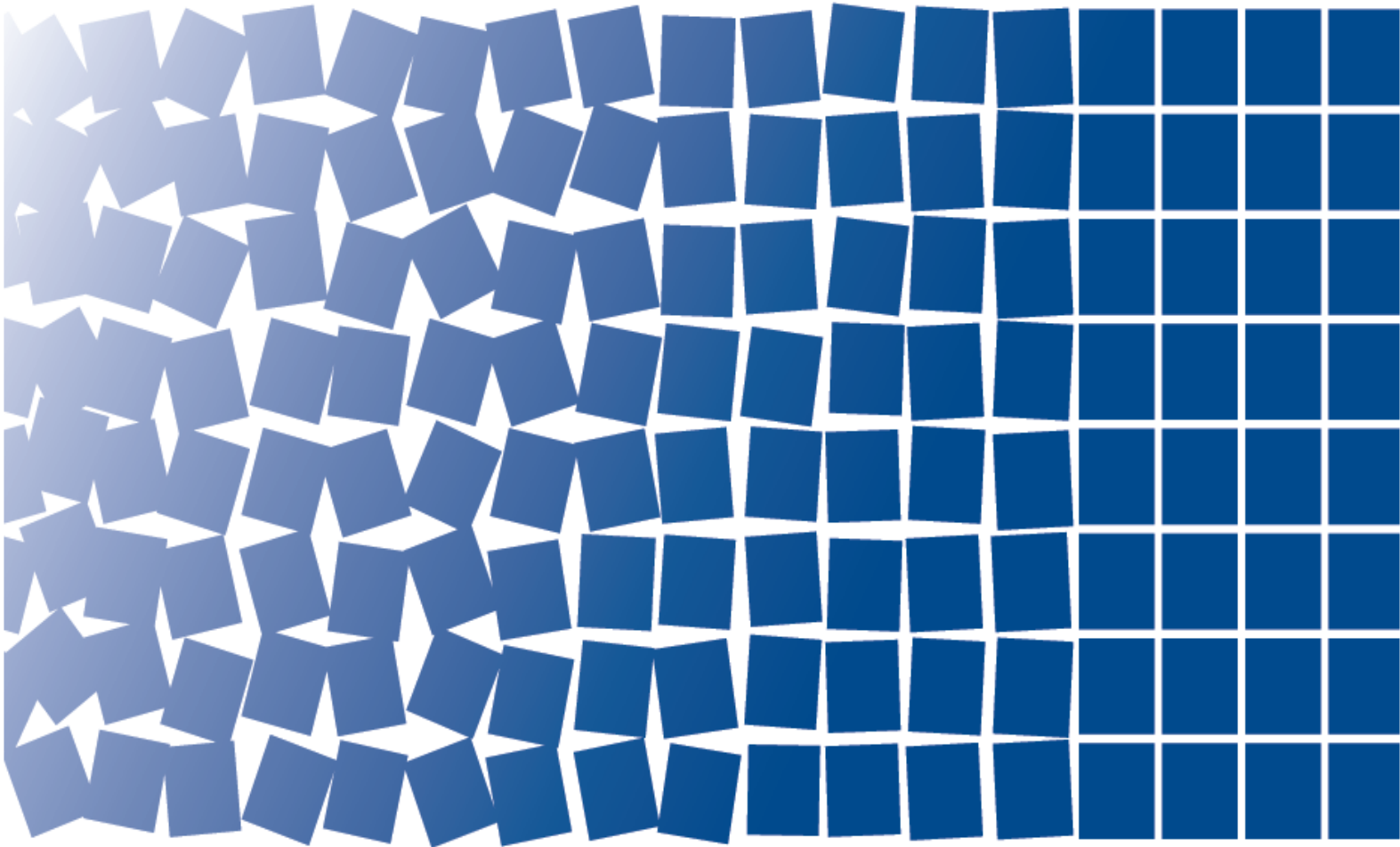
This Quick Reference Guide is intended to provide staff with immediate access to key points associated with the *Freedom of Information and Protection of Privacy Act* (FOIPPA) * of BC.

1. All records in the custody, or under the control of the Trust and Columbia Power Corp (the organizations) are subject to FOIPPA.
2. Records in the custody of a contractor, delivery partner, or service provider, and under the control of the organizations, are subject to FOIPPA.
3. All records are subject to access requests under FOIPPA (including relevant transitory* records that exist at the time of the request).
4. Many of the organizations' records are routinely available to the public, proactively provided, and do not require a formal FOI request.
5. Staff should accommodate reasonable access requests to non-confidential and non-personal information ***in an informal way*** wherever possible.
6. Requests for access to another person's personal information or to any confidential information are subject to exceptions in FOIPPA. The Privacy Officer (Senior Manager, Information Services) must be contacted if a formal request for records in writing has been made - privacy@ourtrust.org
7. The organizations have a ***duty to assist*** FOI applicants and must respond to formal FOI requests within 30 business days.
8. Personal information refers to "recorded information about an identifiable individual" and does not include business contact information*.
9. The organizations must only collect personal information if it ***is necessary to fulfill identified purposes and be reasonable and appropriate.***
10. Personal information collected may only be used for the purposes identified when it was collected.
11. An approved collection statement ***must be included*** on forms whenever personal information is being collected by the organizations or by delivery partners.
12. The organizations must make reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, or disposal of personal information.
13. A Privacy Impact Assessment (PIA) ***must be conducted*** on a new initiative, or before implementing a significant change to an existing initiative.
14. A completed corporate PIA covers the use of our in-house grant and program application system.
15. Any suspected or known privacy breach must be reported to the Privacy Officer immediately – privacy@ourtrust.org.

* Additional information is provided under the Privacy section of the Intranet:
https://ourtrust.sharepoint.com/departments/infoservices/Pages/rm_privacy.aspx

Publicly available records pg 93 - 169

COLUMBIA POWER OPERATIONAL RECORDS CLASSIFICATION SYSTEM



GOVERNMENT RECORDS SERVICE

INFORMATION SCHEDULE APPROVAL

Title: *Columbia Power Corporation Operational Records Classification System (ORCS)*

Columbia Power Corporation

Scope of Schedule:

The *Columbia Power Corporation Operational Records Classification System (ORCS)* establishes a classification system and retention and disposition schedule for the operational records created by the Columbia Power Corporation.

The schedule covers records relating to hydro-electric dam construction in the Columbia Basin and ongoing operations and maintenance; dam safety, public safety, and environment, health, and safety; environment and land management; permit and license acquisition; corporate governance; business development; contract management; regulatory affairs; and stakeholder engagement.

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: 1994

The government body endorses this schedule and its implementation.

Authorization on file

Frank Wszelaki, President and CEO, Columbia Power Corporation

October 14, 2015

Date

The Information Management Advisory Committee recommends this schedule for approval.


David Curtis, Chair

June 28/17
Date

APPROVED BY THE CHIEF RECORDS OFFICER:



Cheryl Wenczel, Yolland
David Curtis

Sept 8, 2017
Date

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: Sarah Jensen

Endorsed by Government Records Service.


Alex Wright, Sr. Director
Date

June 28, 2017

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

Columbia Power Corporation

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

EXECUTIVE SUMMARY

This *Operational Records Classification System (ORCS)* establishes an information schedule for the operational records created by Columbia Power Corporation (Columbia Power) pursuant to the *Dam Safety Regulation* (BC Reg. 40/2016), the *Water Users' Communities Act* (RSBC 1996, c. 483), the *Environmental Assessment Act* (SBC 2002, c. 43, s. 17), the *Heritage Conservation Act* (RSBC 1996, c. 187), the *Workers Compensation Act* (RSBC 1996, c. 492, s. 119), the *Fisheries Act* (RSC 1985, c. F-14), and related occupational health and safety regulations.

These records document hydro-electric dam construction in the Columbia Basin and ongoing operations and maintenance; dam safety, public safety, and environment, health and safety; environment and land management; permit and licence acquisition; corporate governance; business development; debt financing; contract management; regulatory affairs; and stakeholder engagement.

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

This *ORCS* covers records created and received since Columbia Power was formed in 1994, as well as a small subset of records that were transferred from BC Hydro to Columbia Power in 1998 as part of an Asset Transfer Agreement.

The following summary describes the records covered by this *ORCS* and identifies their retention periods and final dispositions. In this summary, records are linked to the *ORCS* by primary and secondary numbers. Please consult relevant primaries for further information.

- 1) Policy and procedures
(secondaries 80000-00, 80150-00, 80200-00, 80475-00) SO 5y FR

Throughout this *ORCS*, the government archives will fully retain final versions of all policies, procedures, standards and guidelines having corporate-wide significance and those relating to dam safety, environment, health and safety management, and public safety created by offices having primary responsibility for their development and approval. These records have significant evidential value for documenting the functions covered by this *ORCS*.

- 2) Emergency Preparedness Plan (EPP) and major incidents and deficiencies
(secondaries 80150-05, 80150-25) SO 7y FR

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

These records document Columbia Power's emergency response planning process and management of major incidents and deficiencies.

These records will be retained for seven years after the file has been closed, in accordance with the *BC Dam Safety Regulation* (BC Reg. 163/2011).

The government archives will fully retain these records to document Columbia Power's emergency response planning process and to demonstrate corrective actions have been taken to address major incidents and deficiencies.

- | | | | | |
|----|---|----|----|----|
| 3) | <u>Contaminated sites, heritage investigations, and land management files</u>
(secondaries 80200-25, 80200-45, 80250-20) | SO | 5y | FR |
|----|---|----|----|----|

These records document contaminated sites containing hazards to the public, the findings of archaeological site investigations, and Columbia Power's overall property management practices.

The government archives will fully retain these records as they document hazards to the public for which the government has long term obligations and accountability. They also provide a record of archaeological sites not to be disturbed by dam construction projects. Finally, they offer evidence of Columbia Power's land management activities which may significantly impact the environment over the long-term.

- | | | | | |
|----|---|----|----|----|
| 4) | <u>Operations, Maintenance, and Surveillance (OMS) manuals</u>
<u>Operations and Maintenance (O&M) and engineering manuals</u>
(secondaries 80150-08, 80450-30) | SO | 5y | FR |
|----|---|----|----|----|

These records consist of OMS and O&M manuals.

The government archives will fully retain these manuals as they document Columbia Power's overall dam safety site management practices and provide evidence of the operation and maintenance of Columbia Power's assets and facilities.

- | | | | |
|----|---|-----------|----|
| 5) | <u>Government's letter of expectation</u>
(secondary 80050-35) | CY+1y nil | FR |
|----|---|-----------|----|

These records document the government's letter of expectation to Columbia Power.

The government archives will fully retain these documents because they provide evidence of Columbia Power's mandate and the government's annual direction to the corporation.

- | | | | | |
|----|--|----|-----|----|
| 6) | <u>Record drawings</u>
(secondary 80450-20) | SO | nil | FR |
|----|--|----|-----|----|

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

This secondary consists of record drawings, commonly called as-built drawings, and related specifications as constructed or as modified.

The government archives will fully retain these records as they document the final set of drawings upon completion of a dam construction project, as well as modifications made to the drawings, capturing the effects of operational activities and adverse conditions on operational projects.

- | | | | | |
|----|---|----|-----|----|
| 7) | <u>Dam safety reviews</u>
(secondary 80150-22) | SO | 10y | SR |
|----|---|----|-----|----|

These records document the dam safety review process.

The 10-year semi-active retention period is based on the requirements of the *BC Dam Safety Regulation* (BC Reg. 163/2011) which stipulates a dam safety review and a dam safety report must be completed every seven to ten years depending on the dam's downstream consequence classification.

The government archives will fully retain final review and audit reports because these provide a comprehensive summary of Columbia Power's dam safety standards and practices. All other drafts and working documents may be destroyed when their technical information is no longer relevant to future reviews.

- | | | | | |
|----|---|----|----|----|
| 8) | <u>Dam safety program files</u>
(secondary 80150-03) | SO | 7y | SR |
|----|---|----|----|----|

These records document Columbia Power's process for complying with government regulation and for ensuring the objectives set out in Columbia Power's Dam Safety Policy are achieved.

The government archives will fully retain each final, approved dam safety program document to provide a record of Columbia Power's planned response to unusual dam conditions so potentially hazardous situations can be brought under control and damages avoided. All drafts and working documents may be destroyed.

- | | | | | |
|----|---|----|----|----|
| 9) | <u>Environmental management plans and environmental program files</u>
(secondaries 80200-35, 80200-40) | SO | 7y | SR |
|----|---|----|----|----|

These records document the plans Columbia Power develops and follows to ensure the environment is protected during the management and/or implementation of new projects, as well as programs and projects developed out of commitments or perceived need such as regulatory requirements outlined in applicable legislation.

The government archives will fully retain final, approved environmental management plans for major projects because they provide evidence of Columbia Power's approach to assessing and monitoring the effects of power

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

projects on the natural environment. In addition, they document Columbia Power's compliance with the *Water Act* (RSBC 1996, c. 483) and the *Environmental Management Act* (SBC 2003, c. 53). Environmental management plans for minor or abandoned projects will be destroyed.

The government archives will fully retain final, approved environmental program reports because they provide evidence Columbia Power is complying with applicable regulatory requirements of the BC Environmental Assessment Office (EAO). All other documents and working materials may be destroyed.

- | | | | |
|---|----|----|----|
| 10) <u>First Nations case files</u>
(secondary 80525-20) | SO | 7y | SR |
|---|----|----|----|

These records document Columbia Power's engagement with the First Nations.

The government archives will fully retain case files documenting involvement of First Nations in Columbia Power's power project investments because they provide evidence of compliance with the *Haida Nation v. British Columbia* (Minister of Forests) Supreme Court decision stating government is legally obligated to consult with First Nations on land or resource decisions which may impact aboriginal interests. These records possess historical and evidential value. All working copies and draft documents may be destroyed.

- | | | | |
|---|----|----|----|
| 11) <u>Construction project files</u>
(secondary 80325-20) | SO | 6y | SR |
|---|----|----|----|

These records document the initiation, identification, definition, execution, and closure of construction projects.

The government archives will selectively retain construction project files because they provide evidence of Columbia Power's management of construction projects. Selected files will include final project /evaluation reports detailing the history and development of the project, appended design drawings, and other project-related records documenting major decisions and events not required for ongoing operational purposes. Records appraised for destruction include routine project management documentation, drawings and copies of technical documents, and the records of projects that cease to progress or are abandoned. All other documents, drafts, and working materials may be destroyed.

- | | | | |
|--|----|----|----|
| 12) <u>Board minute books files and audits</u>
(secondaries 80050-20, 80150-20, 80200-20, 80450-25) | SO | 5y | SR |
|--|----|----|----|

These records document the board minute books files of Columbia Power's executive, as well as records relating to internal and third party audits.

The government archives will fully retain material case files (the final issued board package) and approved minute books, containing copies of Columbia

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

Power's charter documents, as they provide a complete record of board deliberations and decisions. All other documents, drafts, and working materials may be destroyed.

The government archives will fully retain final audit reports performed by external auditors and completed corrective action plans because they demonstrate due diligence. These records have significant informational and evidential value. All other drafts and working documents may be destroyed.

- 13) Inspection reports SO 10y DE
(secondary 80150-35)

These records document weekly, monthly, and semi-annual/annual dam safety inspection reports.

The ten-year semi-active retention period provides a sufficient period of time to ensure Columbia Power's due diligence obligations are met.

- 14) Corporate tax returns FY+1y 6y DE
(secondary 80025-20)

The records consist of copies of income tax returns filed on behalf of Columbia Power and the joint venture companies.

The retention period ensures these records are available to taxation authorities, which have the right under the *Income Tax Act* (RSC 1985, c. I-5, ss. 230(4) and 231.1) to investigate income tax returns filed for the previous six years.

- 15) Systems SO nil DE

The Systems Section provides descriptions of electronic systems and classifications for the records residing on them. The data on the systems are described under the appropriate primary and secondary classifications.

Unless otherwise noted, each system will be destroyed when the records/data on it have been migrated to a new system performing the same function, or when the relevant retention schedules have elapsed, or the information has been preserved elsewhere.

- 16) 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 the ORCS or in ARCS, such as summary reports, policy records, executive briefing notes (ARCS secondary 280-20), and

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information, consult your [Records Officer](#).

A SA FD

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

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

USEFUL INFORMATION

Key to Information Schedule Codes and Acronyms:

Information Schedule titles:	ARCS = <i>Administrative Records Classification System</i> ORCS = <i>Operational Records Classification System</i>
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.](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A

SA

FD

SECTION 1

COLUMBIA POWER CORPORATION

PRIMARY NUMBERS

80000 - 89999

Section 1 covers records relating to the activities of the Columbia Power Corporation (Columbia Power) pursuant to the *Dam Safety Regulation* (BC Reg. 40/2016), the *Water Users' Communities Act* (RSBC 1996, c. 483), the *Environmental Assessment Act* (SBC 2002, c. 43, s. 17), the *Heritage Conservation Act* (RSBC 1996, c. 187), the *Workers Compensation Act* (RSBC 1996, c. 492, s. 119), the *Fisheries Act* (RSC 1985, c. F-14), and occupational health and safety regulations. This includes records relating to dam construction, operations, and maintenance; dam safety, public safety, and environment, health and safety; environment and land management; permit and licence acquisition; corporate governance; business development; debt financing; contract management; regulatory affairs; and stakeholder engagement.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

SECTION 1

80000 – COLUMBIA POWER CORPORATION - 89999

TABLE OF CONTENTS

80000	COLUMBIA POWER CORPORATION - GENERAL
80025	CORPORATE GOVERNANCE - GENERAL
80050	- BOARD OF DIRECTORS AND INCORPORATION
80100	BUSINESS DEVELOPMENT
80150	DAM SAFETY
80175	DEBT FINANCING
80200	ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT
80250	LAND MANAGEMENT
80275	PERMITS AND LICENCES
80300	PROCUREMENT AND CONTRACT MANAGEMENT
80325	PROJECTS - CONSTRUCTION
80400	PUBLIC SAFETY
80450	OPERATIONS AND MAINTENANCE
80500	REGULATORY AFFAIRS
80525	STAKEHOLDER RELATIONS AND COMMUNICATIONS

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80000 COLUMBIA POWER CORPORATION – GENERAL

Records not shown elsewhere in this ORCS relating to the operational activities of the Columbia Power Corporation (Columbia Power). Its primary mandate is to efficiently develop and operate commercially viable, environmentally sound and safe power projects for the benefit of the province and the residents of the Columbia Basin.

Record types include: correspondence, memoranda, and reports.

Unless otherwise specified below, the Columbia Power OPR (Columbia Power) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	FR
		- <u>non-OPR</u>	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO = when the policy or procedure is replaced or no longer required for reference purposes

FR = The government archives will fully retain final versions of operational policy documentation because these provide significant evidence of the governance of the functions and services covered by this section.

-01 General

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80025 CORPORATE GOVERNANCE - GENERAL

Records not shown elsewhere in the corporate governance section that relate generally to the establishment and executive leadership of the Columbia Power Corporation (Columbia Power) or its joint venture companies.

Record types include: correspondence, memoranda, and reports.

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

For board of directors, see primary 80050.

For final policies of corporate-wide significance, see secondary 80000-00.

For incorporation materials, see primary 80050.

Unless otherwise specified below, the Columbia Power OPR (Columbia Power) will retain these records for:

CY+1 nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00 Policy and procedures

- OPR

SO 5y DE

- non-OPR

SO nil DE

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-20 Corporate tax returns

FY+1y 6y DE

(arrange by year)

(covers copies of income tax returns filed on behalf of Columbia Power and the joint venture companies)

8y: The retention period ensures these records are available to taxation authorities, which have the right under the *Income Tax Act* (RSC 1985, c. I-5, ss. 230(4) and 231.1) to investigate income tax returns filed for the previous six years.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80050 CORPORATE GOVERNANCE - BOARD OF DIRECTORS AND INCORPORATION

Records relating to the activities and composition of the board of directors of the Columbia Power Corporation (Columbia Power) and associated joint venture companies.

This primary also includes records relating to the incorporation of Columbia Power and to the establishment of joint venture and other partnership companies.

Record types include: agendas, manuals, minutes, correspondence, memoranda, and reports.

For agreements, see ARCS primary 146.

For budget estimates, see ARCS primary 1000.

For committees other than the Board of Directors, see ARCS secondary 200-20.

For executive briefings, see ARCS primary 280.

For final policies of corporate-wide significance, see secondary 80000-00.

For financial statements, see ARCS secondary 1180-20.

For Treasury Board submissions, see ARCS primary 1250.

For updates to the minister, see ARCS primary 280.

Unless otherwise specified below, the Columbia Power OPR (Columbia Power) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00 Policy and procedures

- OPR

SO

5y

DE

- non-OPR

SO

nil

DE

(covers reference copies of records from BC Government's Board Resourcing and Development Office)

SO: when the policy or procedure is replaced or no longer required for reference purposes

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80050 CORPORATE GOVERNANCE - BOARD OF DIRECTORS AND
INCORPORATION (continued)

-01 General

-02 Board binder development
(covers materials prepared for submission to the
board)

NOTE: Board binder material that is approved for
presentation to the board is reclassified to
secondary 80050-20.

PIB -05 Board membership files SO 5y DE
(arrange by name)
(covers board member biographies, performance
appraisals, requests and approval of board
member appointments, indemnity agreements,
code of ethics, conflict of disclosure statements,
credit checks, remuneration, appointment checklist
forms)

SO: when no longer a member of the board

NOTE: These files are created for the Board Resourcing
and Development Office which approves all
appointments to the Columbia Power board.

-07 Board manuals SO 5y DE
(includes orientation material and the board
procedures manual)

SO: when there is a significant update to the manual

-08 Board updates CY+5y nil DE
(covers interim correspondence to board members,
primarily updates from Columbia Power)

-09 Board tracking
(covers tracking of meeting attendance and the
remuneration paid to board members, a
requirement for government compliance)

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

			<u>A</u>	<u>SA</u>	<u>FD</u>
80050	<u>CORPORATE GOVERNANCE - BOARD OF DIRECTORS AND INCORPORATION</u> (continued)				
VR	-20	Board minute books files (includes minute books, calendars work plans, and material case files which are the final issued board package) (arrange by meeting date)	SO	5y	SR
		SO: when the board is no longer active or records are no longer required for reference purposes			
		SR: The government archives will fully retain approved minute books and material case files, containing copies of Columbia Power's charter documents, as they provide a complete record of board deliberations and decisions. All other documents, drafts, and working materials may be destroyed.			
	-35	Government's letter of expectation (arrange by year) (covers the annual letter of expectation as delivered by the minister responsible for Columbia Power and related correspondence)	CY+1y	nil	FR
		FR: The government archives will fully retain letters of expectation because they provide the government's annual direction to the corporation and set Columbia Power's mandate.			

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

SECTION 1 - 8

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80100 BUSINESS DEVELOPMENT (continued)

NOTE: If the potential project progresses beyond an initiation phase to board approval and project planning, relevant portions of the project file are re-classified to primary 80325 or the relevant project/program secondary.

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

SECTION 1 - 10

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80150 DAM SAFETY (continued)

- SO: when the program is updated and no longer required for reference purposes
- 7y: The seven-year semi-active retention period ensures the records are available for a sufficient period of time for program planning, monitoring, and evaluation purposes.
- SR: The government archives will fully retain each final, approved dam safety program document to provide a record of Columbia Power's planned response to unusual dam conditions so potentially hazardous situations can be brought under control and damages avoided. All drafts, planning/research materials, and working documents may be destroyed.

- | | | | | |
|-----|--|----|----|----|
| -05 | Emergency Preparedness Plan (EPP) files
(arrange by asset)
(covers records relating to the Emergency Response Plan (ERP) and the Emergency Preparedness Guide (EPG) which comprise the EPP) | SO | 7y | FR |
| | SO: when replaced by a new plan that has been accepted by the dam safety officer | | | |
| | 7y: The seven-year semi-active retention period is based on the requirements of the <i>BC Dam Safety Regulation</i> (BC Reg. 40/2016). | | | |
| | FR: The government archives will fully retain final versions of the EPP for their evidential and informational values. These records document Columbia Power's approach to emergency response planning which is in compliance with government regulation. | | | |
| -08 | Operations Maintenance and Surveillance (OMS) manuals
(includes draft and final/approved OMS manual)
(arrange by asset)
(covers records relating to the operations, maintenance and surveillance of the facility) | SO | 5y | FR |

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80150 DAM SAFETY (continued)

SO: when replaced with a new manual which has been reviewed and approved by the dam officer

FR: The government archives will fully retain the final/approved manuals as they provide evidence of Columbia Power's overall dam safety site management practices, in accordance with government regulation.

-09 Security measures files - dams SO 5y DE
(includes reports, drafts, assessments, and the Site Security Management plan)
(arrange by asset)
(covers records relating to topics such as potential vandalism, terrorism, security breaches, and other security concerns associated with the management of the dams)

SO: when no longer required for purposes of dam security

-20 Audits SO 5y SR
(includes internal or third party audits)
(arrange by date, then topic)

SO: when any resulting corrective action has been taken and verified

SR: The government archives will fully retain final audit reports performed by external auditors and completed corrective action plans because they demonstrate due diligence. These records have significant informational and evidential value. All other drafts and working documents may be destroyed.

-22 Dam safety reviews SO 10y SR
(includes reports, reviews, checklists, correspondence, terms of reference)
(arrange by asset, then by date)
(covers records relating to the dam safety analysis process)

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80150 DAM SAFETY (continued)

SO: when a new report is complete and has been approved by the dam safety officer and is no longer required for reference purposes

10y: The 10-year semi-active retention period is based on the requirements of *the BC Dam Safety Regulation* (BC Reg. 40/2016) which stipulates a dam safety review and a dam safety report must be completed every seven to ten years depending on the dam's downstream consequence classification.

SR: The government archives will fully retain final review and audit reports because these provide a comprehensive summary of Columbia Power's dam safety standards and practices. All other drafts and working documents may be destroyed when their technical information is no longer relevant to future reviews.

-25	Incidents and deficiencies - major (includes photos, reports, assessments, design reviews) (arrange by asset, then by topic or incident number) (covers major incidents or deficiencies identified by inspections, the remedial action taken to reconcile them, as well as design reviews and considerations such as details of unique components of design structures)	SO	7y	FR
-----	--	----	----	----

SO: when the incident or deficiency is resolved or for the lifespan of the asset

7y: The seven-year semi-active retention period is consistent with dam safety review requirements under the *Dam Safety Regulation* (BC Reg. 40/2016).

FR: The government archives will fully retain records documenting major incidents and deficiencies in order to demonstrate corrective actions have been taken and to offer a complete maintenance record. Columbia Power is required by government regulation to safely operate and maintain its dams and related water conveyance works.

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80150	<u>DAM SAFETY</u> (continued)			
-30	Incidents and deficiencies - minor (includes monthly surveillance checklists, photos, reports, and assessments) (arrange by asset, then topic or incident number) (covers minor incidents or deficiencies identified by inspections and the remedial action taken to reconcile them) SO: when the incident or deficiency is resolved 7y: The seven-year semi-active retention period is consistent with dam safety review requirements under the <i>Dam Safety Regulation</i> (BC Reg. 40/2016).	SO	7y	DE
-35	Inspection reports (includes weekly, monthly, semi-annual/annual reports) (arrange by asset, then by date) (covers records relating to inspections including reports prepared by the dam owner) SO: when the latest annual report is generated and no longer required to demonstrate due diligence 10y: The ten-year semi-active retention period provides a sufficient period of time to ensure Columbia Power's due diligence obligations are met. DE: Inspection reports may be destroyed because records covering major incidents or deficiencies identified by inspections are fully retained in secondary 80150-25.	SO	10y	DE
-45	Monitoring data (arrange by asset, then by date) (covers data gathered from surveillance instrumentation and physical surveillance) SO: when the asset or system is replaced, discontinued or decommissioned	SO	nil	DE

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80150 DAM SAFETY (continued)

NOTE: Water levels are monitored by the Historian or Management Information System (MIS) and ground movement is measured by surveyors using surveillance equipment.

-50	Monitoring instrumentation (includes specifications and surveillance equipment issues) (arrange by asset, then equipment type)	SO	2y	DE
	SO: when the instrument is replaced or its use is discontinued			

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80175 DEBT FINANCING

Records relating to the raising of funds to support capital expenditures/investments by issuing bonds to institutional investors or by borrowing directly from the province in the form of fiscal agency loans. In return for lending the money, the institutional investors become creditors and receive a promise (such as a deed of trust) that the principal and interest on the debt will be repaid. For borrowing from the province, a debenture will be issued. A debenture is an unsecured loan as the province is the sole shareholder of Columbia Power.

Record types include: correspondence, memoranda, and reports.

For final policies of corporate-wide significance, see secondary 80000-00.

For power sales agreements, see ARCS secondary 146-45.

For regulatory affairs, see primary 80500

For trust deed, see ARCS secondary 146-45.

Unless otherwise specified below, the corporation OPR (Finance) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	DE
		- non-OPR	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-02	Investor contact list	SO	nil	DE
-----	-----------------------	----	-----	----

SO: when outdated or no longer relevant

-20	Bond sale marketing files (arrange by bond issuance date) (covers records relating to the development of the offering memoranda, independent advisor reports, presentation materials, and agency rating analysis)	SO	7y	DE
-----	---	----	----	----

SO: when the bond is issued
(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80175 DEBT FINANCING (continued)

7y: The seven-year semi-active retention period is a reasonable period of time to ensure no potential issues with the investors arise.

-25	Bondholder reporting package (arrange by year) (covers quarterly financial statements, as well as compliance and insurance certificates mailed to registered bondholders)	FY	2y	DE
-----	---	----	----	----

-35	Commercial debt financing case files (includes line of credit) (arrange by asset)	SO	5y	DE
-----	---	----	----	----

SO: when the debt is paid or the account is closed

-40	Financing plan development files (includes correspondence, financing plan, drafts, spreadsheets, and research materials) (covers records documenting the development of the financing strategy/plan, part of the capital financing requirement, which is submitted to Treasury Board)	SO	5y	DE
-----	---	----	----	----

SO: when the financing plan is accepted by Treasury Board

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80200 ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT

Records relating to Columbia Power Corporation (Columbia Power)'s corporate approach to environment and health and safety management.

Environmental management includes environmental monitoring through environmental programs and remediation activities as required by the Environmental Assessment Certificate issued under the *Environmental Assessment Act* (SBC 2002, c.43, s.17) and water licences as issued under the *Water Users' Communities Act* (RSBC 1996, c. 483). This primary also includes heritage investigations pursuant to the *Heritage Conservation Act* (RSBC 1996, c. 187) and other records pursuant to applicable provincial and federal environmental legislation such as the *Fisheries Act* (RSC 1985, c. F-14).

Records relating to health and safety management practices include incident management, policy and procedure development, reporting, and investigations pursuant to the *Canada Labour Code Part 2, Workers Compensation Act* (RSBC 1996, c. 492, s.119), *Occupational Health and Safety Regulation* (BC Reg. 296/97), and *BS Occupational Health and Safety Standard (OHSAS) 18001:2007*. These records document Columbia Power's responsibilities as a facility owner of safe and healthy workplaces.

Record types include: correspondence, memoranda, and reports.

For dam safety, see primary 80150.

For a description of the Environmental Health and Safety Requirements Database (EHSRD), see the Systems Section.

For employee occupational safety, health and accidents, see *Human Resources ARCS Supplement* primary 7560.

For environmental assessment certificates, see primary 80275.

For Joint Occupational Safety and Health (JOSH) committee, see *ARCS* primary 200.

For land management, see primary 80250.

For public safety, see primary 80400.

For water licences, see primary 80275.

Unless otherwise specified below, the corporation OPR
(Environment and Health & Safety) will retain these records for: CY+1y nil DE

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80200 ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT (continued)

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	FR
		- <u>non-OPR</u>	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO: when the policy or procedure is replaced or no longer required for reference purposes

FR: The government archives will fully retain final versions of operational policy documentation because these provide significant evidence of the governance and functions and services covered by this section.

-01 General

VR	-02	Corrective action log (covers records relating to required corrective actions identified in audits, incidents, and inspections)	SO	3y	DE
----	-----	--	----	----	----

SO: when the log is replaced or the function is discontinued

VR	-03	Environmental Health and Safety Management System (EHS_MS) files (includes master control log and table of contents, manual, blank forms, templates, drafts, and other supporting documents)	SO	3y	DE
----	-----	---	----	----	----

SO: when replaced with a new system

NOTE: For final, approved versions of the EHS_MS manual, see secondary 80200-00.

VR	-08	Risk assessments (includes completed forms)	CY	5y	DE
----	-----	--	----	----	----

NOTE: Risk assessments are reviewed and updated annually.

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80200	<u>ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT</u> (continued)			
-20	Audits (includes correspondence, images, scope development documentation, drafts, final reports, and action plans) (arrange by year and/or project) (covers records relating to EHS compliance audits, prepared internally or by third parties) SO: when all resulting corrective actions have been completed and verified SR: The government archives will fully retain final audit reports performed by external auditors and completed corrective action plans because they demonstrate Columbia Power was exercising due diligence by performing regular environmental and health and safety audits and correcting any deficiencies flagged in the audits. These records have significant informational and evidential value. All other drafts and working documents may be destroyed. NOTE: The corrective action log is classified under secondary 80200-02.	SO	5y	SR
-25	Contaminated sites files (includes waste manifest, investigation files, site risk classification report, and notice of independent remediation) (arrange by asset, Parcel Identification (PID) number, or topic) (covers records relating to contaminated sites investigations such as initial notification, recommendations for remediation, and other remediation related activities) SO: when a site is no longer considered active and/or a certificate of completion is received	SO	5y	FR

(continued on next page)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80200 ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT

(continued)

FR: The government archives will fully retain files on contaminated sites because they document hazards to the public for which the government has long term obligations and accountability. Contaminated sites files provide evidence of significant environmental impact caused by dams owned and operated by Columbia Power.

VR	-35	Environmental management plans (arrange by asset, then by date) (covers records relating to the plans Columbia Power follows to ensure the environment is protected during the management and/or implementation of new projects)	SO	7y	SR
----	-----	--	----	----	----

SO: when the project is complete

7y: The seven-year semi-active retention period is consistent with the retention period of contracts which outline the contractors' commitment to follow the plan during construction.

SR: The government archives will fully retain final, approved environmental management plans for major projects because they provide evidence of Columbia Power's approach to assessing and monitoring the effects of power projects on the natural environment. In addition, they document Columbia Power's compliance with the *Water Users' Communities Act* (RSBC 1996, c. 483) and the *Environmental Management Act* (SBC 2003, c. 53). Environmental management plans for minor or abandoned projects will be destroyed.

VR	-40	Environmental program files (includes terms of reference, issues, correspondence, monitoring data, and final reports) (arrange by program or project name) (covers records relating to programs and projects developed out of commitments or perceived need such as regulatory requirements outlined in applicable legislation)	SO	7y	SR
----	-----	--	----	----	----

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80200 ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT

(continued)

- SO: when the program/project is complete and/or with agreement from the regulators (i.e. Ministry of Environment, Fisheries and Oceans Canada)
- 7y: The seven-year semi-active retention period is a sufficient period of time to ensure risk to the environment is mitigated and all regulatory requirements are met.
- SR: The government archives will fully retain final, approved environmental program reports because they provide evidence Columbia Power is complying with applicable regulatory requirements of the BC Environmental Assessment Office (EAO). These records have evidential and informational value. All other documents and working materials may be destroyed.

NOTE: For periodic inspections, not part of an environmental program, see secondary 80200-55.

-45	Heritage site investigation case files (arrange by site name or investigation type) (covers records relating to archaeological site investigations)	SO	5y	FR
-----	---	----	----	----

- SO: when the heritage site investigation is complete
- FR: The government archives will fully retain heritage site investigation case files since they document the findings of archaeological site investigations, revealing sites not to be disturbed by dam construction projects in compliance with the *Heritage Conservation Act* (RSBC 1996, c. 187).

NOTE: Copies of the investigation reports are delivered to the relevant government office such as Ministry of Forests, Lands and Natural Resource Operations.

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80200	<u>ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT</u> (continued)			
-50	Incident management case files (includes incident logs, metrics, reports, and tracking documentation) (arrange by log type, then by year and incident number) (covers records relating to Columbia Power, contractor, and regulator EHS and incident reports including initial notification, investigation, non-conformance, and recommendations for corrective action) SO: when the incident is resolved, corrective action has been taken, and no longer required for reference purposes DE: These records may be destroyed as significant EHS incidents are adequately documented under secondary 80500-20 Board minute books files and special schedule 102906 (<i>Executive Records</i>), which are selectively retained. NOTE: For incidents relating to Columbia Power employees, see ARCS secondary 1560-20.	SO	6y	DE
-55	Inspection files (includes images, reports, and correspondence) (covers periodic EHS inspections, as well as monitoring reports conducted by Columbia Power, contractors, and regulators) SO: when the inspection is complete and any resulting corrective actions have been closed and verified	SO	6y	DE
-60	Issues management case files (arrange by topic and/or project) (covers proactive exploration of potential or real areas of concern) SO: when the issue is resolved and no longer required for reference purposes	SO	5y	DE

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80200	<u>ENVIRONMENT, HEALTH AND SAFETY MANAGEMENT</u> (continued)			
-65	Health and safety program files (includes first aid needs assessment, training program materials, correspondence, monitoring data, and final reports) (arrange by asset, then by topic) (covers records relating to Columbia Power owned/developed and contractor developed Environmental and Health and Safety programs)	SO	7y	DE
	SO: when the health and safety program is updated and no longer required for reference purposes			
	7y: The seven-year semi-active retention period meets Columbia Power's due diligence obligations, mitigates potential risks, and ensures the records are available for program planning, monitoring, and evaluation purposes.			
	NOTE: For environmental program files, see secondary 80200-40.			
-75	Environmental Health and Safety Requirements Database (EHSRD) (includes electronic database and related records/reports)	SO	nil	DE
	SO: when no longer used as an index to relevant commitments or no longer required for reference purposes			
	DE: This electronic system can only be destroyed when the approved retention periods covering the information on it have elapsed, or when the information on it has been made accessible elsewhere.			

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

SECTION 1 - 25

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80250 LAND MANAGEMENT (continued)

(covers records relating to access agreements, acquisition negotiations, appraisals, expropriations, land exchanges and compensations for fee simple, rights of way, easements, history of any impacts or transactions occurring during Columbia Power's tenure, disposal negotiations, and transfer agreements)

SO: when the interest in the property is extinguished and all outstanding commitments are met

FR: The government archives will fully retain land management files as they document Columbia Power's property management practices relating to acquisition, disposal, maintenance, and access rights. They also provide evidence of the use of land for activities that may significantly impact the environment over the long-term.

NOTE: Information related to detection of contamination of sites and associated remediation is classified under secondary 80200-25.

-30	Geographical Information System (GIS) data (covers spatial data such as orthographic photographs acquired from the provincial government and/or purchased from private entities relating to the lands and assets owned or managed by Columbia Power for use in projects)	SO	nil	DE
-----	---	----	-----	----

OPR: Operations and Environment

SO: when GIS data is no longer required for reference purposes or when the agreement with the service provider is altered or terminated

NOTE: The GIS data is stored and made accessible to Columbia Power staff by an offsite service provider.

NOTE: This secondary is not for filing. It is used for classifying data on an external hard drive housed at Columbia Power and the data stored by the offsite service provider for the duration of the agreement.

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80275 PERMITS AND LICENCES

Records relating to the acquisition of authorizations such as water licences and project approval certificates, now referred to as environmental assessment certificates, by Columbia Power Corporation (Columbia Power) or its joint venture companies.

Record types include: permits, licences, correspondence, memoranda, and reports.

For agreements, see ARCS secondary 146-45.

For final policies of corporate-wide significance, see secondary 80000-00.

For radio frequency licences, see ARCS primary 6890.

For software licences, see ARCS primary 737.

Unless otherwise specified below, the corporation OPR (originating office) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00 Policy and procedures

- OPR

SO

5y

DE

- non-OPR

SO

nil

DE

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-20 Permit/licence development files
(includes correspondence, applications, reports, and studies)
(arrange by asset, then by name)
(covers the development of application submissions for permits and licences)

SO

5y

DE

SO: when the application is rejected or discontinued and the information is not required for renewal or reference purposes

-45 Permits/licences

(includes final issued permits and licences)
(arrange by asset, then by name)

SO

5y

DE

SO: when the permit or licence expires
(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80300 PROCUREMENT AND CONTRACT MANAGEMENT

Records relating to the development and establishment of contracts. This primary includes contracts to procure goods, services, and construction in compliance with the *Core Policy and Procedures Manual* and the *Standards of Conduct for Public Service Employees Engaged in Government Procurement Processes*.

Record types include: registers, contracts, correspondence, memoranda, solicitation documents, and reports.

For accounts payable, see ARCS primary 925.

For agreements, see ARCS primary 146.

For final policies of corporate-wide significance, see secondary 80000-00.

Unless otherwise specified below, the corporation OPR (Procurement and Contracts) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	DE
		- <u>non-OPR</u>	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-03	Contract register (arrange by subject)	SO	nil	DE
-----	---	----	-----	----

SO: when register is no longer required and/or all referenced contracts are closed or discontinued

VR	-20	Contract files (includes correspondence, contract negotiation documents, drafts, operating orders, owners' requirements, final contract change orders, and contract amendments) (arrange by contract name or number)	SO	7y	DE
----	-----	--	----	----	----

SO = upon expiry or termination of the contract or upon audit or other requirements stipulated in the contract
(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80300 PROCUREMENT AND CONTRACT MANAGEMENT (continued)

7y: The seven-year semi-active retention period is based on the need to research the previous contract's activities during contract re-negotiation, ensures the records are available for fiscal accountability, and provides a reasonable period of time for the legal value of the records to be extinguished.

-30	Procurement files (includes Requests for Information (RFI), Requests for Proposals (RFP), tenders, Requests for Quotes (RFQ), and related correspondence) (arrange by contract name or number) (covers records relating to procurement activities such as technical details, financing documents, proposals, assessments, and evaluations)	SO	7y	DE
-----	---	----	----	----

SO: when the contract is signed or the solicitation process ends

7y: The seven-year semi-active retention period is based on the need to research the previous contract's activities during contract re-negotiation, ensures the records are available for fiscal accountability, and provides a reasonable period of time for the legal value of the records to be extinguished.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80325 PROJECTS - CONSTRUCTION

Records relating to the initiation, identification, definition, execution/implementation, and closure of projects such as construction projects carried out by Columbia Power Corporation (Columbia Power), either on its own or through a joint venture or partnership.

Record types include: correspondence, memoranda, reports, and other types of records indicated under relevant secondaries.

For contract details, see primary 80300.

For environmental programs, see secondary 80200-40.

For final policies of corporate-wide significance, see secondary 80000-00.

For IT projects, see ARCS secondary 6450-20.

For ministry planning and projects, see ARCS secondary 400-20.

For operations and maintenance, see primary 80450.

For records and information management (RIM) projects, see ARCS secondary 432-60.

Unless otherwise specified below, the corporation OPR (Project Management Office) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00 Policy and procedures

- OPR

SO 5y DE

- non-OPR

SO nil DE

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-20 Construction projects files

SO 6y SR

(includes drawings, technical documents, correspondence, presentations, photographs, news clippings, reports, meeting materials, project management materials, operational documents such as manuals, training materials, and standard operating procedures)
(arrange by project name)
(covers records relating to project initiation, identification, definition, execution, and closure)

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80325 PROJECTS - CONSTRUCTION (continued)

SO: when the project ceases to progress or final acceptance has been achieved and the warranty obligations as per the contract are completed and no longer required for reference purposes

SR: The government archives will selectively retain construction project files because they provide evidence of Columbia Power's planning and management of construction projects. Selected files will include final project/evaluation reports detailing the history and development of the project, appended design drawings, and other project-related records documenting major decisions and events not required for ongoing operational purposes.

Records appraised for destruction include routine project management documentation, drawings and copies of technical documents, and the records of projects that cease to progress or are abandoned. All other documents, drafts, and working materials may be destroyed.

NOTE: For ongoing operations and maintenance, see primary 80450.

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

SECTION 1 - 32

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80400	<u>PUBLIC SAFETY</u> (continued)			
-01	General			
-03	Public safety management plan (PSMP) files (includes drafts, plans, drawings, maps, and correspondence) (covers the set of procedures and controls established to ensure the safety of the public around hazardous water control works) SO: when the plan is updated or no longer required for safety purposes DE: These records may be destroyed as final, approved public safety management plan manuals are fully retained in secondary 80400-00.	SO	5y	DE
-20	Control measures (arrange by asset, then by name and year) (covers records relating to controls used to promote public safety including signage, signals, barriers, and changes to operations)			
-25	Incident management case files (includes initial notification and investigation files, and recommendations for remediation) (arrange by year, then by incident number) (covers records relating to incidents involving the public) SO: when any investigation as a result of an incident is complete and any claims are resolved NOTE: Insurance claims resulting from incidents will be classified under ARCS secondary 450-20.	SO	6y	DE
-35	Public safety inspection reports (arrange by asset, then by date) (covers records relating to inspections reports) SO: when the inspection is completed and any resulting follow up steps are completed	SO+1y	6y	DE

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80400 PUBLIC SAFETY (continued)

7y: The combined 7-year active and semi-active retention periods provide a sufficient period of time to meet Columbia Power's due diligence obligations.

DE: These records may be destroyed as procedures for inspection and maintenance of the physical installations are adequately documented in the approved PSMP, secondary 80475-00.

-40	Public safety risk assessments (arrange by asset, then by year) (covers records relating to the public safety risk assessment process following the structured approach of the Canadian Dam Association (CDA) <i>Dam Safety Guidelines</i>)	SO	5y	DE
-----	--	----	----	----

SO: when risk to the public has been mitigated, due diligence has been demonstrated, and risk mitigation has been implemented

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80450 OPERATIONS AND MAINTENANCE

Records relating to the management of hydroelectric facilities and transmission facilities managed by the Columbia Power Corporation (Columbia Power).

Record types include: manuals, correspondence, drawings, memoranda, and reports.

For a description of the Historian system, see the Systems Section.

For equipment not identified by an equipment system number, see *ARCS* primary 700.

For final policies of corporate-wide significance, see secondary 80000-00.

Unless otherwise specified below, the corporation OPR (Operations) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00 Policy and procedures

- OPR

SO

5y

DE

- non-OPR

SO

nil

DE

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-02 Asset management program development files
(includes strategies, plans, drafts, and working documents)

SO

5y

DE

(covers records relating to the development of the asset management program, particularly in relation to the effects of operations on CPC assets)

DE: These records may be destroyed as final, approved versions of asset management documentation are fully retained under secondary 80000-00.

VR -05 Recommended action log

SO

3y

DE

(covers records relating to corrective actions identified in audits, events, or inspections)

SO: when the log is no longer maintained

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

			<u>A</u>	<u>SA</u>	<u>FD</u>
80450	<u>OPERATIONS AND MAINTENANCE</u> (continued)				
VR	-20	Record drawings (arrange by Equipment System number, see Appendix A) (covers record drawings, commonly called as-built drawings, and related specifications as constructed or as modified) SO: when the equipment is replaced or disposed of FR: The government archives will fully retain record drawings of operational assets such as dams and transmission lines as they document the final set of drawings upon completion of a dam construction project, as well as modifications made to the drawings which capture the effects of operational activities and adverse conditions on operational projects.	SO	nil	FR
	-25	Audits (includes internal or third party audits) (arrange by date, then by topic) SO: when any resulting corrective action has been taken and verified SR: The government archives will fully retain final audit reports performed by external auditors and completed corrective action plans because they demonstrate due diligence. These records have significant informational and evidential value. All other drafts and working documents may be destroyed.	SO	5y	SR
VR	-30	Operations and Maintenance (O&M) and engineering manuals (includes commissioning manual, facility manual, commissioning reports, test results, installation manuals, quality control testing results, and alignment records) (arrange by Equipment System number, see Appendix A) SO: when the equipment is replaced or disposed of (continued on next page)	SO	5y	FR

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80450 OPERATIONS AND MAINTENANCE (continued)

FR: The government archives will fully retain these manuals as they provide evidence of the operation and maintenance of Columbia Power's assets and facilities.

-50 Operating instructions SO 5y DE
(includes Local Operating Orders (LOO), Joint Operating Orders (JOO), System Operating Orders (SOO) and ad hoc procedural instructions)

SO: when the equipment is replaced or disposed of

VR -55 Operational equipment history SO 5y DE
(arrange by equipment system number, see Appendix A)
(covers records relating to acquisition, maintenance, operation and disposal information of component equipment, as well as outstanding construction deficiencies, and/or warranty issues)

SO: when the equipment is replaced or disposed of

NOTE: If a complex response is required by Columbia Power to mitigate the effects of negative events on operational equipment, an operations and maintenance project may be initiated. The resulting records are classified under secondary 80450-65.

-65 Operations and maintenance projects SO 6y DE
(arrange by project)
(covers records created in response to significant events, risk reduction, or capitalizing on an opportunity)

SO: when the project ceases to progress or when the project is complete

NOTE: Project documentation that has ongoing significance for the operation of component equipment is re-classified to the operational equipment history file under secondary 80450-55.

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

		<u>A</u>	<u>SA</u>	<u>FD</u>
80450	<u>OPERATIONS AND MAINTENANCE</u> (continued)			
-70	Reporting (arrange by report type) (covers records relating to regulatory reporting and reporting according to agreements about Columbia Power's equipment) SO: when the equipment is replaced and disposed of and/or when the reporting agreement is closed	SO	5y	DE
-75	Water management files (includes flow forecasts, notifications received from operators, and resulting analysis documents) SO: when no longer required to substantiate current water flow entitlement for future development agreements or for water use planning activities NOTE: Changes to the operations of facilities as a result of water management activities will be reflected in operating instructions which are classified under secondary 80450-50.	SO	6y	DE

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80500 REGULATORY AFFAIRS

Records relating to monitoring and consulting on Columbia Power Corporation (Columbia Power)'s regulatory requirements. This primary includes research into proposed legislative or regulatory changes and review of the provisions of the Columbia River Treaty.

Record types include: correspondence, memoranda, and reports.

For environment, health and safety management, see primary 80200.

For final policies of corporate-wide significance, see secondary 80000-00.

Unless otherwise specified below, the corporation OPR (Commercial Contracts and Regulatory) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	DE
		- <u>non-OPR</u>	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-02	Regulatory research files	SO	nil	DE
-----	---------------------------	----	-----	----

SO: when the research is completed or discontinued and no longer required for reference purposes

-20	Regulatory review files (includes review materials, reports, analysis, and correspondence) (arrange by topic) (covers records relating to monitoring and intervening in regulatory hearings of affiliated agencies (i.e. Fortis BC, BC Hydro) or hearings on tax policy or water hearings)	SO	nil	DE
-----	---	----	-----	----

SO: when no longer required for reference purposes

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80525 STAKEHOLDER RELATIONS AND COMMUNICATIONS

Records relating to Columbia Power Corporation (Columbia Power)'s communications and engagement with corporations, local government, special interest groups, First Nations, and the general public.

Record types include: correspondence, memoranda, and reports.

For agreements, see ARCS primary 146.
 For committees, see ARCS primary 200.
 For complaints, see ARCS primary 155.
 For corporate communications, see ARCS primary 295.
 For environmental assessment certificates, see primary 80275.
 For events, see ARCS primary 220.
 For final policies of corporate-wide significance, see secondary 80000-00.
 For image bank, see ARCS primary 306.
 For incidents, see secondary 80200-50.
 For inquiry logs, see ARCS primary 320.
 For issues, see secondary 80200-60.
 For marketing and advertising, see ARCS primary 295.
 For media relations, see ARCS primary 330.
 For operations and maintenance, see primary 80450.
 For planning documents, see ARCS primary 400.
 For signage, see ARCS primary 295.
 For web sites, see ARCS primary 340.

Unless otherwise specified below, the OPR (Stakeholder Relations and Communications) will retain these records for:

CY+1y nil DE

Except where non-OPR retention periods are identified below, all other corporation offices will retain these records for:

SO nil DE

-00	Policy and procedures	- OPR	SO	5y	DE
		- <u>non-OPR</u>	<u>SO</u>	<u>nil</u>	<u>DE</u>

SO: when the policy or procedure is replaced or no longer required for reference purposes

-01 General

-20	First Nations case files (includes correspondence, photographs, presentations, meeting materials, research materials, and logs) (continued on next page)	SO	7y	SR
-----	--	----	----	----

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80525 STAKEHOLDER RELATIONS AND COMMUNICATIONS (continued)

(arrange by name of First Nation and/or the project as appropriate)

- SO: when the consultation/project is complete and any agreements and associated commitments have been met or are closed
- 7y: The seven-year semi-active retention period provides a sufficient period of time for any concerns with the consultation process/project to arise
- SR: The government archives will fully retain case files documenting involvement of First Nations in Columbia Power's power project investments because they provide evidence of compliance with the *Haida Nation v. British Columbia* (Minister of Forests) Supreme Court decision stating government is legally obligated to consult with First Nations on land or resource decisions which may impact aboriginal interests. These records possess historical and evidential value. All working copies and draft documents may be destroyed.

-40 Scholarship files CY+1y nil DE
 (arrange by year, then by name of educational institution)
 (covers records relating to criteria and awarding of scholarships)

-45 Sponsorships FY+1y 5y DE
 (includes applications, correspondence, photographs, presentations, and thank you notes)
 (arrange by year, then by organization)
 (covers the awarding of sponsorships to the local community by Columbia Power)

7y: The seven-year retention period provides a reasonable period of time to identify issues and resolve anomalies and is consistent with the retention period for similar financial records classified in ARCS.

(continued on next page)

[Key to ARCS/ORCS Codes and Acronyms](#)

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

A SA FD

80525 STAKEHOLDER RELATIONS AND COMMUNICATIONS (continued)

-50	Stakeholder relations case files (includes correspondence, photographs, and presentations) (arrange by name of stakeholder group, then by project as appropriate) (covers records relating to stakeholder consultations about corporate operations, facilities management, project development, and construction)	SO	7y	DE
	SO: when the consultation/project is complete			
	7y: The seven-year semi-active retention period provides a sufficient period of time for any concerns with the consultation process/project to arise.			
	DE: These case files may be destroyed as records documenting significant involvement of local communities in major power project investments are adequately documented in ARCS secondary 146-45.			

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

Columbia Power Corporation

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

SYSTEMS SECTION TABLE OF CONTENTS

<u>SECTION AND TITLE</u>	<u>PAGE NO.</u>
COMMON SYSTEM NOTES	2
Environmental Health and Safety Requirements Database (EHSRD)	3
Historian or Management Information System (MIS)	5

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. 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.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

ENVIRONMENTAL HEALTH AND SAFETY REQUIREMENTS DATABASE (EHSRD)

SYSTEM OVERVIEW

Name of Creating Agency

Columbia Power Corporation (Columbia Power)

System Title

Environmental Health and Safety Requirements Database (EHSRD)

Purpose

The EHSRD tracks commitments and obligations established for both environmental and health and safety concerns (EHS). Licenses, permits, and agreements (foundation documents) result in a variety of commitments or obligations for Columbia Power, as project manager, to fulfill. The EHSRD lists these commitments, attributing them to the individual responsible, the current status (e.g. open, closed, and expired), the company or project. The EHSRD does not, however, include the general requirements of environmental or health and safety legislation.

Note that the EHSRD is used to track both environmental and health and safety requirements as they are part of Columbia Power's integrated Environment, Health and Safety Management System (EHS_MS).

The EHSRD was developed to keep track of Columbia Power's environmental requirements, and provide access to the specific requirements within those documents quickly and easily. The health and safety aspect was added later when the integrated EHS_MS was developed. EHS requirements include terms, conditions, and obligations found in contracts, authorizations and approval certificates [e.g., Project Approval Certificate (PAC), now referred to as environmental assessment certificates], as well as contractual and voluntary commitments Columbia Power may have made with landowners or with organizations to which Columbia Power belongs. All such documents that are environmental or health and safety related have been included, whether or not they contain specific requirements, as well as other non-EHS documents that contain EHS requirements.

Information Content

The EHSRD is composed of two relational databases. One is a database of documents; the other is a database of commitments that arise from the documents.

Inputs, Processes, and Outputs

Information is entered and updated manually in the databases. Inputs are links to the cited documents with a summary of the individual commitments and documents via an internal web viewer.

Technical Maintenance

This is an Access 2003 application connected to the EHSRD SQL Server 2005 database.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

Electronic records are maintained on the system until their retention schedule is completed. In most cases, this parallels the schedule for the related paper records.

For retention and disposition schedules, see relevant primaries, which are listed in the classification section below. Also see the system scheduling and disposition section at the end of this ISO.

Classification

Electronic System

Secondary No.
80200-75

Secondary Title
Environmental Health and Safety Requirements Database (EHSRD)

Electronic Records

Inputs

Secondary No.
ARCS 146-45
80275-20
80450-55

Secondary Title
Approved internal and local agreement files
Permit/license development files
Operational equipment history

Outputs

Secondary No.
80200-75

Secondary Title
Environmental Health and Safety Requirements Database (EHSRD)

Other Related Records

- For transitory electronic data processing (EDP) records, see special schedule 102902.
- For computer system backup records, see ARCS secondary 6820-05.
- For administrative records relating to the system, see ARCS section 6 and other relevant primaries.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

SYSTEM OVERVIEW

Name of Creating Agency

Columbia Power Corporation

System Title

"Historian" or "Management Information System (MIS)"

Purpose

"Historian" enables remote (web based) access to historic and real-time monitoring data and reports drawn from monitoring instruments located at the generating stations.

Information Content

The system imports alarms, outage reports, and power generation monitoring from various monitoring devices.

Inputs, Processes, and Outputs

Information is taken from onsite monitoring devices at the generating facilities. It is then formatted into reports which are available for viewing via web browser. Data from individual monitoring points can be viewed as a graph or as a table.

Reports, graphs, tables and raw data can be exported out of the viewer for further analysis and/or use.

Technical Maintenance

Electronic records are maintained on the system until their retention schedule is completed. In most cases, this parallels the schedule for the related paper records. The electronic records are then purged from the system. Any exceptions to this purge routine are noted under relevant secondaries.

For retention and disposition schedules, see relevant primaries, which are listed in the classification section below. Also see the system scheduling and disposition section at the end of this ISO.

Classification

Electronic System

This electronic system is not classified in the ORCS as it is only a tool used to present the information collected from a data logger. The classifications for the electronic records it generates are listed below. The system schedule is provided under "System Scheduling and Disposition".

Inputs

Secondary No.

Secondary Title

Outputs

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

Secondary No.

80450-55

Secondary Title

Operational equipment history

Other Related Records

- For transitory electronic data processing (EDP) records, see special schedule 102902.
- For computer system backup records, see ARCS secondary 6820-05.
- For administrative records relating to the system, see ARCS section 6 and other relevant primaries.

System Scheduling and Disposition

The 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.

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Appendix A

Subject Naming Standards for Operations and Maintenance files

Subject	Equipment System #	Covers	Includes
Cef Filing (Non Equipment Base)	100	O&M Repetitive Job Binders	Repetitive Job Estimate Binders
Site Operations and Maintenance	100	Overhaul Manuals and Annual Inspections Binders	10 year Overhaul Manuals 20 Year Overhaul Manuals Plant Inspection Reports Binders (<i>Electrical</i>) Plant Inspection Reports Binders (<i>Mechanical</i>)
Site Operations and Maintenance	200	Plant or Unit Summary	Aerial site photographs Electrical systems lists Maps Mechanical and electrical systems failure studies Mechanical systems lists Site plans
Site Operations and Maintenance	207	Kootenay Lake Storage	Nelson Gauge
Site Operations and Maintenance	209	Other Operating Costs	Safety Safety supplies Training Equipment Change Request Thermal Imaging 1st Aid Equipment
Site Operations and Maintenance	212	Engineering, Design & Drafting (If separate from other equipment systems)	Prints Engineered lifting Devices Engineered Scaffolding Engineered Pedestals Engineered Calculations
Maintenance of Hydraulic Structures and Equipment	220	Hydraulic Concrete Structures (Wing Dams)	Conduit Embedded pipe and heating cables Flashing Forebay stairways Guardrails Outdoor lighting Plant fencing Power outlets

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Hydraulic Structures and Equipment	221	Spillways	De-icing systems Electrical equipment <i>(heaters, lighting attached to the Sluice Gate super structure, main feeders, motors and controls, outlets, spillway standby generating equipment)</i> Gates Gate hoist equipment Spillway and Sluice Gates super structures Stop logs Standby Generator
Maintenance of Hydraulic Structures and Equipment	222	Intake	Booms and adjustment of booms Electrical equipment <i>(disconnects, lighting, main feeders, motors and controls - See Section 234, outlets)</i> Gates Hoist equipment Intake super structure Penstocks Rail tracks Slot covers Stop logs Trash rack gantry Trash racks
Maintenance of Hydraulic Structures and Equipment	224	Tailrace	Draft tubes <i>(including access manhole)</i> Electrical equipment <i>(main feeders, motors and controls)</i> Rail tracks Slot covers Tailrace gantry Tailrace gates
Maintenance of Hydraulic Structures and Equipment	225	Environmental System	Oil Containment Oil Skimmers
Maintenance of Hydraulic Structures and Equipment	226	Reservoir / Head Pond Shoreline	

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Generating Equipment	230	Turbines	Access to the turbine pit and the scroll case Base ring Greasing wicket gates and associated links and levers Head covers Levers Links Main gland Mercoid controls Operating ring Scroll case Shear pins <i>(including failure indicators)</i> Turbine bearing Turbine runner Vacuum valve Wicket gates Wipe down of turbine equipment and turbine pit well and seal coating pit walls
Maintenance of Generating Equipment	231	Governors	Accumulator and sump tanks Flyball mechanisms Governor Governor oil filter systems and associated electrical equipment <i>(gate limit motor, governor pump motors, governor solenoids gate position micro-switches, mercoid controls, speed adjust motor)</i> Governor piping Governor pumps Permanent magnet generators (PGM) Restoring mechanism Servo-motors Speed switches Unloader valve Wipe down of governing systems and regular lubrication of linkages and motor
Maintenance of Generating Equipment	232	Generators	Air-gap expansion gauges Bearing temperature gauges Brake micro-switches Brake system Fire protection system inside unit enclosure and automatic fire valves <i>(See Sections 234 and 263)</i> Generator shaft <i>(from coupling upwards – including coupling)</i> Hi-pressure oil lift system Neutral grounding equipment Resistance temperature detectors (RTD) of thermocouples Vibro System PDA Protection Shaft oil pump Thrust and guide bearings <i>(including seals)</i>

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Generating Equipment	233	Excitation Systems	Brush assemblies Slip rings Field circuit breaker (where applicable, pilot exciter, magnetic amplifier, amplidyne and rapcon solid state exciter) Field leads Field rheostat Hydraulic water wheel exciters Temperature detectors
Maintenance of Generating Equipment	234	Control Systems	Cable cooling control Fire annunciation HMI Level controllers Plant controllers Plant cooling control SCADA Security annunciation (not video) Spillway gate positioning Selsyns Unit controllers Generator Control Cabinet Generator Termination Cabinet
Maintenance of Generating Equipment	235	Lubricating Systems	Automatic grease systems and all associated electrical equipment (pump motors and controls, mercoird controls, oil flow switches, pressure gauges) Filter systems Lubricating oil pumps Piping Replacement oil Sump tanks Wipe down of lubricating system piping and equipment as required and cost of processing lubricating oil
Maintenance of Generating Equipment	236	Cooling Water Systems	Air wash system (air chambers, air wash fan, filters, motors and controls, nozzles, pumps) Forebay well cooling water supply Generator bearing cooling water system (where applicable, the unifin (radiator) cooling system and associated filters, piping and valves), automatic shut-off solenoids, bearing cooling coils, flow switches, piping to generator guide and thrust bearing, water filters)
Maintenance of Generating Equipment	237	Generator Switchgear	Cable cooling fans (where applicable) Circuit breakers Indoor generator disconnects Lightning arrestors Surge capacitors Transformer connection

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Plant Auxiliary Equipment	240	Protective Relays	Metering Protective relaying Relay CT's and PT's
Maintenance of Plant Auxiliary Equipment	241	Data Collection Systems	GPS clock Inter-utility data exchange Meters Totalizers
Maintenance of Plant Auxiliary Equipment	242	AC Station Service	120 AC distribution panels <i>(associated supply cables and conduit)</i> 550 Volt welding outlets and associated conduit and cabling 600 Volt station service switchgear or bus work <i>(as applicable)</i> 2300 Volt station service circuit breakers Branch circuits <i>(up to and including main disconnects and circuit breakers)</i> <i>(Excludes 2300V transmission lines - See Section 257)</i> Main and auxiliary station service supply cables and raceways Station service and lighting transformers and voltage regulators
Maintenance of Plant Auxiliary Equipment	243	DC Station Service	Battery chargers DC distribution panels Motor generator (MG) sets, where applicable Plant emergency lighting and all associated cable and conduit Storage batteries
Maintenance of Plant Auxiliary Equipment	244	Cranes, Hoists and Elevators	Auxiliary hoist equipment and all associated electrical equipment Crane rails and power supply conductors Elevators Motors and controls Power house Power supplies Roof cranes
Maintenance of Plant Auxiliary Equipment	245	Sump Pumps and Dewatering Systems	Electrical equipment <i>(controls, power supplies, pump motors)</i> Piping Sump pumps Unwatering pumps Valves
Maintenance of Plant Auxiliary Equipment	246	Compressed Air Systems	Brake compressor Compressed air supply piping De-icing compressors and blowers Electrical equipment <i>(motors and controls, power supplies)</i> Gauges General service air compressor Hi-Air compressor Turbine head cover blowers Valves

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Plant Auxiliary Equipment	247	HVAC Systems, Cable Cooling Systems	220 Volt heater outlets 550 Volt heaters Air conditioning equipment Air supply exhaust All building heating and ventilating equipment Circulating fans Generating unit ventilating system Roof vents Tailrace filters Winter cooling floor filters
Maintenance of Plant Auxiliary Equipment	248	Communication Networks Hardware	JMUX multiplexor Microwave Plant fibre and communication cabling Telus fibre Transmission Video systems (security and safety) Voice system
Maintenance of Plant Auxiliary Equipment	249	Miscellaneous Shop Tools and Equipment	Consumable tool supplies (drill bits, files, saw blades, etc.) Shop tools and equipment Tool replacement (under \$100 each)
Maintenance of Switchyard	250	Generator Step-Up Transformers	Conservator tank Gas relay Generator transformers High voltage (HV) and low voltage (LV) connectors and bushings Processing of transformer oil Radiators and fans (if applicable)
Maintenance of Switchyard	251	Transmission Transformers	Conservator tank Gas relay High voltage (HV) and low voltage (LV) connectors and bushings Processing of transformer oil Radiators and fans (if applicable)
Maintenance of Switchyard	252	High Voltage Circuit Breakers	Built-in compressor Bushings Control panels Oil and air circuit breakers (generating unit and transmission line) Receiver systems
Maintenance of Switchyard	253	Switchyard (If separate from plant)	Fire protection systems Lightning arrestors Potential transformers Surge capacitors Transformer cooling water system Transmission line instrument transformers
Maintenance of Switchyard	254	Switchyard	Disconnect switches (manual and motor operated) Switching station bus work

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Switchyard	255	Switchyard Structure and Grounds	Buildings inside switchyard Fences Handrails Rail tracks Station grounding Super structures Switchyard foundations
Maintenance of Switchyard	256	Switchyard Lighting and AC Services	Power outlets Switchyard lighting
Maintenance of Switchyard	257	Transmission Lines	230 kV line from Arrow Lakes Hydro to Brilliant terminal station Fibre optic cables High voltage transmission lines P1 to P4 inter-plant 60 kV and 2300 V lines
Maintenance of Buildings, Structures and Services	258	Power Distribution	Poles, wires at distribution level Tieline Transformers for distribution
Maintenance of Buildings, Structures and Services	260	Buildings and Structures	Benches Buildings and associated out buildings Doors Furniture Handrails Seal-coating of floors and walls Shelving Windows Power House
Maintenance of Buildings, Structures and Services	261	Sewer and In-Plant Water Systems	Fixtures associated with sewer and domestic water systems Motors and controls Piping Pumps Valves
Maintenance of Buildings, Structures and Services	262	Domestic Water Supply Systems	Canals Dams Sluice gates Valves Water mains
Maintenance of Buildings, Structures and Services	263	Fire Systems	Fire detection and protection systems (<i>excepting the switchyard</i>) at power plants Fire extinguishers Fire pumps Generator sprinkler systems (<i>as applicable</i>) Hydrants and hoses Motors and controls Piping Valves
Maintenance of Buildings, Structures and Services	264	Janitorial and Garbage	Disposal of waste oil and lubricants Janitorial and garbage disposal services Janitorial supplies
Maintenance of Buildings, Structures and Services	265	Roads, Gates and Fences and Bridges	Access roads Main gates Security fencing

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

In accordance with the [Information Management Act](#) (SBC 2015, c. 27), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. Consult your [Records Officer](#).

Subject	Equipment System #	Covers	Includes
Maintenance of Buildings, Structures and Services	266	Gardens and Grounds	Lawns Railway spur lines Sidewalks Yards
Maintenance of Buildings, Structures and Services	267	Snow Removal	Replacement of snow shovels Snow removal Snow removal equipment
Maintenance of Buildings, Structures and Services	268	Materials Handling	Staff and General Roll time <i>(associated with stock record preparation)</i> Warehousing activities
Maintenance of Buildings, Structures and Services	269	Leased Vehicle Rentals	Rental payments
Maintenance of Buildings, Structures and Services	271	Vehicle Operations and Maintenance	Gas Oil Repairs
Cef Filing (Non Equipment Base)	800	Insurance Information	Insurance Inspections <i>(Filed in Binders)</i> Insurance Information <i>(Filed in File Folders & Pockets)</i> Reference Information <i>(Filed in File Folders & Pockets)</i>

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

COLUMBIA POWER CORPORATION

OPERATIONAL RECORDS CLASSIFICATION SYSTEM (ORCS)

INDEX

This index provides an alphabetical guide to ORCS subject headings and relevant primary number(s). It should enable the user to locate the primary number(s) in which documents relating to a specific subject or function may be classified. It should also aid the user in retrieving, by subject, documents which have been classified and filed.

Employees responsible for records classification should use this index as a means of access to the contents of ORCS. Once they have located what appear to be relevant index entries for a given subject, they should refer to the primary or primaries listed in order to determine which is the correct classification and also to determine the correct secondary. Often, the primary scope notes will clarify whether or not a document should be classified in a given primary. Primary scope notes should be read carefully as they delineate a primary's subject and content.

This index contains an alphabetical listing of:

- a) all keywords which appear in primary titles;
- b) all keywords which appear in secondary titles;
- c) keywords which appear in primary scope notes;
- d) common synonyms for indexed keywords; and
- e) 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.

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

- A -

AS-BUILT DRAWINGS	(See RECORDS DRAWINGS)	
ACCIDENT		
- health and safety		80200
- public safety		80400
ACQUISITION		
- land		80250
- equipment		80450
ACTION LOG (See LOGS)		
AGENDA		
- board of directors		80050
AGREEMENTS		
- board of directors		80050
- land		80250
ANALYSIS		
- business development		80100
- dam safety		80150
- finance		80175
- operations		80450
- regulatory affairs		80500
APPRAISALS		
- board of directors		80050
- land		80250
ASSET MANAGEMENT		80450
AUDIT		
- dam safety		80150
- environment		80200
- health and safety		80200
- contracts		80300
- operations and maintenance		80450

- B -

BOARD OF DIRECTORS	80050
BONDS	80175
BUSINESS DEVELOPMENT	80100

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

BUSINESS OPPORTUNITIES (See BUSINESS DEVELOPMENT)

- C -

CERTIFICATES	
-environmental assessment	80275
-insurance	80175
CHANGE ORDERS	80300
COMMERCIAL DEBT FINANCING	80175
COMMISSIONING MANUALS (See MANUALS)	
COMMITMENTS	
- health and safety	80200
- environment	80200
- land	80250
COMMUNICATIONS	
- stakeholder relations	80525
COMPENSATION	
- land	80250
CONSTRUCTION CONTRACTS (See CONTRACTS)	
CONSULTATIONS	80525
CONTAMINATED SITES	
- environment	80200
CONTRACT FILES (See CONTRACTS)	
CONTRACTOR	
- health and safety	80200
CONTRACTS	80300
CONTROL MEASURES	
- public safety	80400
CORPORATE FILINGS	80025
CORPORATE GOVERNANCE	80050
CORRESPONDENCE LOG (See LOGS)	

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

- D -

DAM SAFETY	80150
DEBT FINANCING	80175
DEFICIENCIES	
- dam safety	80150
- environment	80200
- health and safety	80200
- operations	80450
DISPOSAL	
- land/property	80250
- operations	80450

- E -

EASEMENTS	
- land/property	80250
EMERGENCY PREPAREDNESS PLAN (EPP)	
- dam safety	80150
ENGINEERING MANUALS (See MANUALS)	
ENVIRONMENTAL AUDIT (See AUDITS)	
ENVIRONMENTAL HEALTH AND SAFETY REQUIREMENTS DATABASE (EHSRD)	80200
ENVIRONMENTAL HEALTH AND SAFETY MANAGEMENT SYSTEM (EHS_MS)	80200
ENVIRONMENTAL MANAGEMENT	80200
ENVIRONMENTAL MONITORING	80200
EQUIPMENT	
- maintenance	80450
- monitoring instrumentation	80150
- operations	80450
EQUIPMENT SYSTEM NUMBER	APPENDIX A
EHSRD	80200
(See also ENVIRONMENTAL HEALTH AND SAFETY REQUIREMENTS DATABASE)	

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

EVENT IDENTIFICATION (See EVENTS)

EVENTS

- maintenance 80450
- operations 80450

EXPROPRIATION

- land 80250

- F -

FACILITY MANUALS (See MANUALS)

FILINGS (See INCORPORATION)

FINANCIAL STATEMENTS

- BONDHOLDER REPORTING 80175

FIRST AID 80200

FIRST NATIONS 80525

- G -

GEOGRAPHICAL INFORMATION SYSTEM (GIS) 80250
Systems section

- H -

HAZARDOUS MATERIAL INFORMATION 80225

HEALTH AND SAFETY

- audits 80200
- compliance issues 80200
- incidents 80200
- incident log 80200
- inspections 80200
- Notices of Projects 80200
- programs 80200
- public safety 80400
- reports 80200
- risk assessments 80200
- safety plans 80200

HERITAGE SITE

- environment 80200

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

HISTORIAN SYSTEM

Systems Section

- I -

INCIDENTS

- communications	
- dam safety	80150
- environment	80200
- health and safety	80200
- operations	80450
- public safety	80400

INCORPORATION

- filings	80050
- materials	80050

INQUIRY LOGS (See LOGS)

INSPECTIONS

- dam safety	80150
- environmental	80200
- health and safety	80200
- operations and maintenance	80450
- public safety	80400

INSTALLATION MANUALS (See MANUALS)

INSURANCE

- certificates	80175
----------------	-------

INVENTORY

- land	80250
--------	-------

INVESTOR

80175

INVOICE

- development	80300
---------------	-------

ISSUES

- board	80050
- environment	80200
- health and safety	80200
- operations and maintenance	80450
- stakeholder relations	80525

- J -

JOINT OPERATING ORDERS (JOOS) (See OPERATING ORDERS)

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

JOOS (See OPERATING ORDERS)

- K -

- L -

LAND

- acquisition	80250
- disposal	80250
- exchanges	80250
- management	80250

LEASE

- land	80250
--------	-------

LETTER OF EXPECTATION 80050

LICENCE 80275

LINE OF CREDIT 80175

LOCAL OPERATING ORDERS (LOOS) (See OPERATING ORDERS)

LOG

- EHS corrective action	80200
- events	80450
- incident	80200
- master control	80200
- recommended action (operations and maintenance)	80450

LOOS (See OPERATING ORDERS)

- M -

MANUALS

- board	80050
- commissioning	80450
- dam safety	80150
- EHS_MS	80200
- engineering	80450
- environment	80200
- facility	80450
- health and safety	80200
- incorporation	80050
- installation	80450
- operations, maintenance, and surveillance manual (OMS)	80150
- operations and maintenance (O&M)	80450
- public safety management plan	80400

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

MARKET RESEARCH	
- opportunities	80100
MARKETING	
- bond sales	80175
MEETINGS	
- projects	80325
- stakeholder relations	80525
MEMBERSHIP	
- board	80050
MONITORING	
- dam safety	80150
- environment	80200
- health and safety	80200
- regulatory affairs	80500

- N -

- O -

O&M MANUALS (See MANUALS)

OPERATING ORDERS	
- contracts	80300
- joint operating orders (JOO)	80450
- local operating orders (LOO)	80450
- system operating orders (SOO)	80450

OPERATIONS, MAINTENANCE, AND SURVEILLANCE
MANUAL (OMS) (See MANUAL)

OPPORTUNITIES (See also BUSINESS DEVELOPMENT)	80100
---	-------

ORIENTATION	
- board members	80050

- P -

PERMITS	80275
---------	-------

PHOTOGRAPHS (See IMAGE BANK)

PROCUREMENT	80300
-------------	-------

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

PROJECTS	
- initiation	80325
- identification	80325
- definition	80325
- execution/implementation	80325
- closure	80325
- opportunity	80100
- development	80100
PROJECT PLANNING	
- opportunities	80100
PROPERTY INVENTORY (See INVENTORY)	
PROPERTY TRANSFER	
- land	80250
PUBLIC SAFETY	80400
- health and safety	80200
- environment	80200
- Q -	
- R -	
RECOMMENDED ACTION LOG (See LOG)	
RECORDS DRAWINGS	80450
REGULATORY AFFAIRS	80500
REGULATORY REVIEW	80500
REPORTS	80000
- board	80050
- corporate governance	80025
- incorporation	80050
REQUESTS FOR PROPOSAL	80300
RESEARCH	
- business development	80100
- financing	80175
- First Nations	80525
- regulatory affairs	80500
RIGHTS OF WAY	
- land	80250

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

RISK ASSESSMENTS

- environment 80200
- health and safety 80200
- public safety 80400

- S -

SAFETY PROGRAMS

- dam safety 80150
- health and safety 80200

SCHOLARSHIP

80525

SECURITY

- dam safety 80150

SHAREHOLDERS

80050

(See also LETTER OF EXPECTATION)

SIGNAGE

- public safety 80400

SOOS (See OPERATING ORDERS)

SPONSORSHIPS

80525

STAKEHOLDER RELATIONS

80525

SUBMITTALS (See PROJECTS)

SURVEILLANCE

(See also SECURITY)

- dam safety 80150

SYSTEM OPERATING ORDERS (SOO) (See OPERATING ORDERS)

- T -

TENURE MANAGEMENT

- land 80250

TESTING

- operations and maintenance 80450

TAX

- corporate tax returns 80025

(continued on next page)

OPERATIONAL CLASSIFICATION SYSTEM

In accordance with the [Information Management Act \(SBC 2015, c. 27\)](#), DO NOT DESTROY ANY RECORDS covered by this information schedule until it has been approved. For more information consult your [Records Officer](#).

TRAINING

- health and safety

80200

- U -

- V -

- W -

WATER MANAGEMENT

- operations

80450

- X -

- Y -

- Z -

Administrative Records Classification System

Last updated on July 24, 2024

Administrative records are common to all offices and are different from operational records. The Administrative Records Classification System (ARCS) is an [information schedule](#) used to classify, file, retrieve and dispose of administrative records.

Search ARCS

Search for ARCS by keyword or file code



Search

ARCS (Schedule 100001) supports business functions like facilities management, property, finance, personnel and information systems, and also includes management functions like committees, contracts and legal activities.

Browse ARCS Primaries

ARCS is organized by business function:

- [Administration \(100 to 499\)](#)
- [Buildings & Properties \(500 to 699\)](#)
- [Equipment & Supplies \(700 to 899\)](#)
- [Financial Management \(900 to 1299\)](#)
- [Human Resource Management \(1300 to 1999\)](#)
- [Information Technology \(6000 to 6999\)](#)

More topics

Resources

Learn how government records are managed:

- [RIM manual](#)
- [RIM glossary](#)
- [Summary of ARCS changes \(PDF\)](#)

Contact information

Contact information for:

- [Ministries](#)
- [Broader Public Sector Organizations](#)



We'd love your feedback!
We have just two questions for you.

