

# Innovate BC

## 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/innovate-bc/>

### 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**

-

## IBC FOIPPA presentation



○ Dawn Wood <dwood@innovatebc.ca>

To: Innovate BC Staff

Friday, July 16, 2021 at 8:56 AM

Hi all,

Thanks for your time Wednesday morning to talk about FOIPPA and Innovate BC.

If you wish to access the powerpoint presentation from this morning, it is saved on the public drive:

Public/bulletin board/Policy Manual and Policies/Info Sessions

[https://innovatebc.sharepoint.com/:p:/s/publicgroup/EV9Pm-5GUEdNoKyciOoFs5wBc-t8VD2A\\_\\_E\\_9wr4oClgbw?e=jbGIR1](https://innovatebc.sharepoint.com/:p:/s/publicgroup/EV9Pm-5GUEdNoKyciOoFs5wBc-t8VD2A__E_9wr4oClgbw?e=jbGIR1)

Thanks!

Dawn

**Dawn Wood**

Director, Compliance + Governance

Innovate **BC**

604 602 5203

Suite 900, 1188 West Georgia St.

Vancouver, BC

[Sign up for our newsletter](#)



# Protection of Privacy

Overview for the Innovate BC team

## Purpose

To provide team with the basic points to help you handle personal information while delivering Innovate BC activities.

There is no longer a single point person for all FOIPPA items.

Director of Marketing will oversee PIAS.

Jennie will delegate other items as they arise.



# This presentation will tell you:

- Definition of personal information
- When and how we may collect, use and share personal information
- Requirements of collecting and holding personal information



- Crown Agency of the Province of BC.
- A public body
- Subject to the Freedom of Information and Protection of Privacy Act (FOIPPA)

# Privacy Legislation

- There is legislation for public bodies and legislation for non-public orgs (eg businesses).
- There is federal legislation.
- Additionally, each province has their own privacy legislation which may be different from one another
- BC's laws for public bodies is called FOIPPA (PIPA for businesses etc)

# Definition of Personal Information

FOIPPA:

Simply put, personal information is any **recorded** information about an identifiable individual other than their business contact information. Personal information includes information that can be used to identify an individual through association or inference.

# Examples of Personal Information

- Name, age, sex
- Home address and phone number
- Race, ethnic origin, sexual orientation
- Number or symbol assigned to the individual
- Education
- Financial information
- Employment information
- Personal views or opinions, except if they are about someone else



## When we can collect personal information

A public body may only collect personal information if it has legal authority to collect it, if the information is for law enforcement purposes or if it is necessary for one of the public body's operating programs.

IBC team: for our use, it is usually 26c or 26e of FOIPPA that applies to our collection of personal information



## FOIPPA Section 26

- A public body may collect personal information only if:
- ...
- (c) the information relates directly to and is necessary for a program or activity of the public body,
- ...
- (e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

## How we may use personal information

A public body may generally only use personal information for the purpose it was collected, for a consistent purpose or with the individual's consent for another purpose.

## How we may share personal information

A public body may only disclose personal information for the purpose it was collected, for a consistent purpose, with the individual's consent or for one of the other specified purposes in the Act, such as law enforcement or to protect individual or public health or safety.

## If we collect personal information we must

- Store data in Canada
- Collect the data directly from the individual
- Post a collection notice
- Complete a Privacy Impact Assessment (PIA)
- Arrange for security of the information
- Strive for accuracy and completeness

## If we collect personal information we must

- Store data in Canada
- If we cannot or prefer not to store data in Canada (eg MailChimp, HubSpot),
  - consider the sensitivity of the information.
  - Obtain consent to store outside of Canada (in collection notice)



## If we collect personal information we must

- Collect the data directly from the individual
  - If we cannot, we must obtain written consent from the individual which authorizes the 3<sup>rd</sup> party to provide that information to us. The consent must tell the individual Innovate BC's purpose for collecting it. (eg DS4Y, VAP)

## If we collect personal information we must

- Post a collection notice
  - The collection notice should be apparent and viewable before the individual submits the information
  - At minimum the collection notice must tell the individual the purpose for collecting their personal information, the legal authorization under FOIPPA for collecting it and provide the business title, address and telephone number of an employee who can answer their questions about the collection.

# If we collect personal information, we must

- Complete a PIA
  - PIAs are a risk mitigation tool. They should be completed before an activity begins. PIAs help us think through the process to ensure we follow the correct steps.
  - Innovate BC PIAs are filed in Operations. You can ask Dir. Mktg for the template and send the completed PIA to Dir. Mktg.
  - PIAs must be kept up to date as program processes change. Most PIAs can be reviewed annually to check for necessary updates.



# If we collect personal information, we must

- Complete a PIA (continued)
  - Examples of PIAs for Innovate BC:
    - Event registration (the process and SaaS tools)
    - Newsletter/mailling list registration
    - Funding programs and related SaaS tools
    - Website
    - Scheduling tools
    - HR records
    - Event tools (eg Zoom)

## If we collect personal information, we must

- Arrange for security of the information
  - Consider the sensitivity of the information, **risk** of unauthorized access, use or disclosure and **effect on the individual** should unauthorized access, use or disclosure occur.
  - Take steps to secure the information accordingly.

## If we collect personal information, we must

- Strive for accuracy and completeness
  - A public body may correct an individual's personal information if the individual requests it and must make a note beside it showing the correction the individual requested



# Freedom of Information

# Freedom of Information Requests

FOI requests are managed by Jennie or Director of Marketing

FOI requests may be made by anyone in the public. For example, media makes requests of public bodies for all sorts of topics, such as approved expenses.

Written records of a public body are subject to an FOI request, including emails, slack threads, Teams chats, even text messages on your personal phone if the texts related to the topic of the FOI request.

These records will become public if they are related to the topic of an FOI request.

It is good practice to maintain professional standards in all messages including internal chats.



## FOIPPA Resources

- Director of Marketing
- Jennie (who may delegate to others)
- Online FOIPPA information
- Privacy Helpline (email and phone) – should be one point person for IBC that contacts Privacy Branch in most cases







**Link:** The training course can be found by clicking this [link](https://order.openschool.bc.ca/Product/Detail/ps_7540006302)  
[https://order.openschool.bc.ca/Product/Detail/ps\\_7540006302](https://order.openschool.bc.ca/Product/Detail/ps_7540006302)

### **How to purchase the course:**

Staff should claim the course fee as an expense and submit their manager-approved expense claim to Finance.

Once you go to the link above, enter the number of course “seats” you want to purchase in the Quantity field. If you are purchasing the course just for yourself, the quantity will be “1”. However, you may be responsible for purchasing the course for multiple individuals in your organization. If this is the case, you can enter the number of courses required in the quantity How to register for the course (for one person)

1. After you’ve paid for the course (either for just yourself or for multiple individuals) an automated email from [osbc.etraining@gov.bc.ca](mailto:osbc.etraining@gov.bc.ca) is sent to you containing a self-registration link. If you are unable to find the email in your inbox, check your junk folder.
2. Open the self-registration link in a web browser.
3. Complete the required fields.

Note: If you have purchased the course for multiple individuals, this step can be carried out in a couple of different ways. Either the self-registration link can be forwarded to each of the individuals required to take the course so that they can register themselves, or one individual can complete the registration process on their behalf and register them one-by-one.

4. Click the Register button.
5. An automated email notifying each registered individual that enrollment is being processed will be sent (within a few minutes of clicking the Register button) from [osbc.etraining@gov.bc.ca](mailto:osbc.etraining@gov.bc.ca).
  1. In this email will be a user ID and password (unique to each registrant).
6. An automated email notifying each registered individual that course enrollment is completed will be sent (within a few minutes after receiving the email in step 5) from [osbc.etraining@gov.bc.ca](mailto:osbc.etraining@gov.bc.ca).
  1. In this email will be a URL where each registered individual can log-in with the user ID and password received in step 5.

### **How to complete the course**

1. Log-in at the following URL: <http://moodle2.openschool.bc.ca>
2. Click on your course title, Privacy and Information Sharing: Awareness Training for Contractors and Service Providers.
3. Open the course material by clicking on the link titled, Privacy and Information Sharing.

4. Read through all the slides.
5. Return to your course home page when you are finished reading the slides.
6. The Certificate link should be available for you to click on.
  1. Open the certificate.
  2. Fill in your name.
  3. Print the certificate.
  4. Once course is completed, generate/Print the Certificate as verification of course completion and send to Finance.

## New Employee Checklist

Employee Name: \_\_\_\_\_

Start Date: \_\_\_\_\_

<input checked="" type="checkbox"/>	ITEM	ACTION	RESPONSIBLE	REFERENCE
<b>Prior to Start</b>				
<input type="checkbox"/>	Welcome Email from CEO	Hiring Manager to provide Ops Manager with new hire information and personal email and request (draft if necessary) to send welcome email	Ops Manager	
<input type="checkbox"/>	Building Access	coordinate security pass/bike storage key Email new employee side door code	Ops Manager/Admin Assistant	Building Access Forms (bike, gym, general)
<input type="checkbox"/>	CEO	book welcome greet with CEO	Ops Manager	
<input type="checkbox"/>	Welcome email with links and forms	compile links of pre-reading , social media accounts and events. Compile PDF copies of HR forms if sending in advance.	Hiring Manager	
<input type="checkbox"/>	Orientation	book small meeting room or office	Hiring Manager	
<input type="checkbox"/>	Calendar	invite new employee to upcoming and re-occurring meetings	Hiring Manager	
<input type="checkbox"/>	Pre Arrival	send out reminder email to staff	Hiring Manager	
<input type="checkbox"/>	Additional Training	organize training for job specific duties	Hiring Manager	
<input type="checkbox"/>	IT Set Up	notify Fulltech new employee name, start date, workstation/laptop printer, Outlook Group add new employee to Microsoft 365 subscription service complete online new employee set up form for FullTech Fulltech to ensure their email signature is set up with their proper title, tele/email info included request user profile for email and login. Fulltech to set up Teams, direct dial nuber and Teams profile Add new employee to Slack	IT Operations FullTech	<a href="#">Complete online new employee setup form for Fulltech</a>
<input type="checkbox"/>	Work Station	ensure all email, folders and logins are working; provide printer codes, User ID & logins add employee's name to printer/copier	IT Operations/Admin Assistant	
<input type="checkbox"/>	Payroll	add new employee to Timesheet	Finance	Timesheet
<input type="checkbox"/>	Credit Card	order travel card/expense cards if required	Finance	Card application form?
<input type="checkbox"/>	Policy Manual	produce or link Innovate BC Policy Manual ensure Code of Conduct has been signed and received (should have come with signed offer)	HR	Policy Manual
<input type="checkbox"/>	Forms	create employee file book time to meet employee and review HR documents, benefits etc. Answer any questions	HR	
<input type="checkbox"/>	Business Cards/Name Tag/Website	order business cards, door plaque, name tag if required add new employee to website	Marketing	

### First Day

<input type="checkbox"/>	Arrival	greet new employee at designated time and location	Hiring Manager	
<input type="checkbox"/>	Orientation Meeting	provide IBC overview issue access cards, business cards, other collect HR documents respond to questions	Hiring Manager Immediate team if required	

<input checked="" type="checkbox"/>	ITEM	ACTION	RESPONSIBLE	REFERENCE
<input type="checkbox"/>	Tour & Introductions	conduct office and building tour (washrooms, lunchroom, recycling, stationery, gym, bike storage and building emergency) and introductions. Explain procedures. Remind to store laptop in locked drawer after hours to avoid theft.	Hiring Manager	
<input type="checkbox"/>	CEO Introduction	Introduce new Employee to CEO; provide CEO swag gifts to present to new employee	Hiring Manager	
<input type="checkbox"/>	Documentation Completion	have employee complete all forms if not completed in advance HR to review forms with employee and answer any questions	HR	
<input type="checkbox"/>	Safety Orientation	HR to review New Worker Safety Orientation	HR (Lily)	Safety Orientation
<input type="checkbox"/>	Timesheet	send timesheet and provide instructions	Finance	
<input type="checkbox"/>	Email	have employee connect to Outlook	Admin Assistant	Style Guide?
<input type="checkbox"/>	Contacts List	provide phone list for the floor and contact info for building management but remind that if it's an emergency they should always dial 911 * coordinate building access documents	Admin Assistant	Floor Contact List
<input type="checkbox"/>	Systems	Instruct employee on system use including logon, filing protocol, access to calendars, printers, phones, login from home, CRM/Salesforce and Slack. Send through FullTech Welcome Package Explain FOIPPA.	IT Operations	Instruction documents

#### First Week

<input type="checkbox"/>	Orientation	continue orientation following up on items not completed first day, ensure all forms and processes (ie timesheets have been completed)	Hiring Manager	
<input type="checkbox"/>	Probation	review job description, review the probation process and form, clearly articulate expectations add probation meetings into Outlook Calendar for you and your new employee introduce the Performance Planning process and share your document	Hiring Manager	Probation Document Copy of Hiring Manager Performance & Performance template
<input type="checkbox"/>	Introductions	conduct additional office introductions if required	Hiring Manager	
<input type="checkbox"/>	Meeting Room & Calendar	conduct training on how to book meetings conduct training on Innovate BC calendar and vacation schedule process	Ops Manager	

#### Fifth Month

<input type="checkbox"/>	Probation	conduct probation review	Hiring Manager	Probation Document
<input type="checkbox"/>	Probation	<a href="#">Staff Training - Privacy and Information Sharing - Online Course</a>	Hiring Manager	See "Link - Privacy" doc

#### Sixth Month

<input type="checkbox"/>	Probation & Performance Planning	confirm appointment and begin PPDP process, identify how to fit employee into the cycle as per the CPC Diagram	Hiring Manager	Performance Planning template HM Performance Plan
<input type="checkbox"/>	Additional Training	both as part of introduction to Performance Planning and ongoing information, identify and action training	Hiring Manager	

# Privacy Impact Assessment for Non-Ministry Public Bodies

## Table of Contents

<b>Before you start</b> .....	1
<b>PART 1: GENERAL INFORMATION</b> .....	2
<b>PART 2: COLLECTION, USE AND DISCLOSURE</b> .....	4
<b>PART 3: STORING PERSONAL INFORMATION</b> .....	6
<b>PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA</b> .....	7
<b>PART 5: SECURITY OF PERSONAL INFORMATION</b> .....	10
<b>PART 6: ACCURACY, CORRECTION AND RETENTION</b> .....	13
<b>PART 7: PERSONAL INFORMATION BANKS</b> .....	15
<b>PART 8: ADDITIONAL RISKS</b> .....	15
<b>PART 9: SIGNATURES</b> .....	16

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in B.C. and are starting a new initiative or significantly changing an existing initiative.

## Before you start

- If you are in a non-ministry public body, you may use this template to document a PIA. This template leads you through a complete PIA, but you are welcome to use another template or method for documenting your PIA
- An initiative is an enactment, system, project, program or activity
- Find information on the [PIA review process](#) and [question-by-question guidance](#)

- If you have any questions, email [Privacy.Helpline@gov.bc.ca](mailto:Privacy.Helpline@gov.bc.ca) or phone [250 356-1851](tel:250-356-1851)

## PART 1: GENERAL INFORMATION

PIA file number:

<b>Initiative title:</b>	
<b>Organization:</b>	
<b>Branch or unit:</b>	
<b>Your name and title:</b>	
<b>Your work phone:</b>	
<b>Your email:</b>	
<b>Initiative Lead name and title:</b>	
<b>Initiative Lead phone:</b>	
<b>Initiative Lead email:</b>	
<b>Privacy Officer:</b>	
<b>Privacy Officer phone:</b>	
<b>Privacy Officer email:</b>	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the [Office of the Information and Privacy Commissioner](#).

**(IBC Note that can be deleted after filling out the form: in IBC's case if we deliver it on our own, the answer to this will always be "no" because— IBC is one body. We are considered as part of the Ministry for the purpose of FOIPPA as a service provider.)**

Yes/No
<p>Is this initiative a common or integrated program or activity? Under section <a href="#">FOIPPA 69 (5.4)</a>, you must submit this PIA to the Office of the Information and Privacy Commissioner.</p> <p><b>(IBC Note that can be deleted after filling out the form: Privacy Officer advised Dawn in the past that most cases are not in this category – if in doubt, check with Privacy Officer)</b></p>
Yes/No
Related PIAs, if any:
List

### 1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

### 2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

### 3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

### 3.1 Did you list personal information in question 3?

**Personal information** is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Type “yes” or “no” to indicate your response.

- If yes, go to [Part 2](#)
- If no, answer [question 4](#) and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

### 4. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

## PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

### 5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.



Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
	Data team to complete this column	Data team to complete this column	Data team to complete this column
Step 1:			
Step 2:			
Step 3:			
Step 4:			

**Optional:** Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

## 6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Review the [sample collection notice](#) and write your collection notice below. You can also attach the notice as an appendix.

**IBC Note that can be deleted after completing this form:**

**FOIPPA legislation requires that public bodies include a “collection notice” whenever we collect personal information and it must include the items listed below.**

**Example notification for collection:**

This information is collected by Innovate BC under [section ??] of the Freedom of Information and Protection of Privacy Act (FOIPPA) and will be used to [purpose]. Should you have any questions about the collection of this personal information please contact

Director, Data + Policy

900 – 1188 West Georgia St

Vancouver, BC V6E 4A2

604-602-5238

## PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

*(IBC Notes to Innovate BC Staff. Please delete after completing the PIA)*

- *FOIPPA legislation requires that public bodies store personal information in Canada. If we must store personal information on servers outside of Canada we must get consent in the correct manner from the individual*
- *The following reply can be used for data stored on Innovate BC server (Question 8 below). This reply was provided by FullTech May 2020):*

Information and data is stored on a cloud server provided by Microsoft, located within Canada. Information can only be accessed outside of Canada by staff should they be travelling for example. Access outside of Canada by employees while travelling is authorized by FOIPPA section 33.1(1)(e).

### 7. Is any personal information stored outside of Canada?

Type "yes" or "no" to indicate your response.

### 8. Where are you storing the personal information involved in your initiative?

### 9. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response.

- If yes, go to [question 10](#)

- If no, go to [Part 5](#)

**10. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?**

Type “yes” or “no” to indicate your response.

- If yes, go to [Part 5](#)
- If no, go to [Part 4](#)

## **PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA**

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization’s Privacy Officer. More help is available in the [Guidance on Disclosures Outside of Canada](#).

**11. Is the sensitive personal information stored by a service provider?**

Type “yes” or “no” to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to [question 13](#)
- If no, go to [question 12](#)

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

**12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.**

**13. Does the contract you rely on include privacy-related terms?**

Type “yes” or “no” to indicate your response.

- If yes, describe the contractual measures related to your initiative.

**15. What controls are in place to prevent unauthorized access to sensitive personal information?**

**16. Provide details about how you will track access to sensitive personal information.**

**17. Describe the privacy risks for disclosure outside of Canada.**

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

### Outcome of Part 4

The outcome of Part 4 will be a **risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

## PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

### 18. Does your initiative involve digital tools, databases or information systems?

Type “yes” or “no” to indicate your response.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of [FOIPPA section 30](#)

#### 18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of [FOIPPA section 30](#)?

Type “yes” or “no” to indicate your response.

- If yes, you may want to append the security assessment to this PIA. Go to [question 20](#)
- If no, go to [question 19](#)

## 19. What technical and physical security do you have in place to protect personal information?

Describe where the digital records for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, you may want to append it to the PIA.

*(IBC Note to user on Physical Security measures: some examples you may wish to include in addition to any others you think of:*

*Information and Data for this program are stored on the cloud, not in physical media.*

*Access to the office requires a door code or key card.*

*Staff log out and physically secure their devices when not in use.)*

*(IBC Note to user on Technical Security measures: the following reply can be used for data stored on Innovate BC server. This reply was provided by FullTech May 2020)*

Innovate BC makes use of a modern firewall, endpoint full disk encryption, and user access accounts are assigned on a need-to-know basis. Innovate BC computers are configured with Mobile Device Management (MDM) that allows for remote lock, data wipe and security compliance enforcement. The Wi-Fi network at Innovate BC is configured with RADIUS to ensure only authorized personnel can access Innovate BC resources and data.

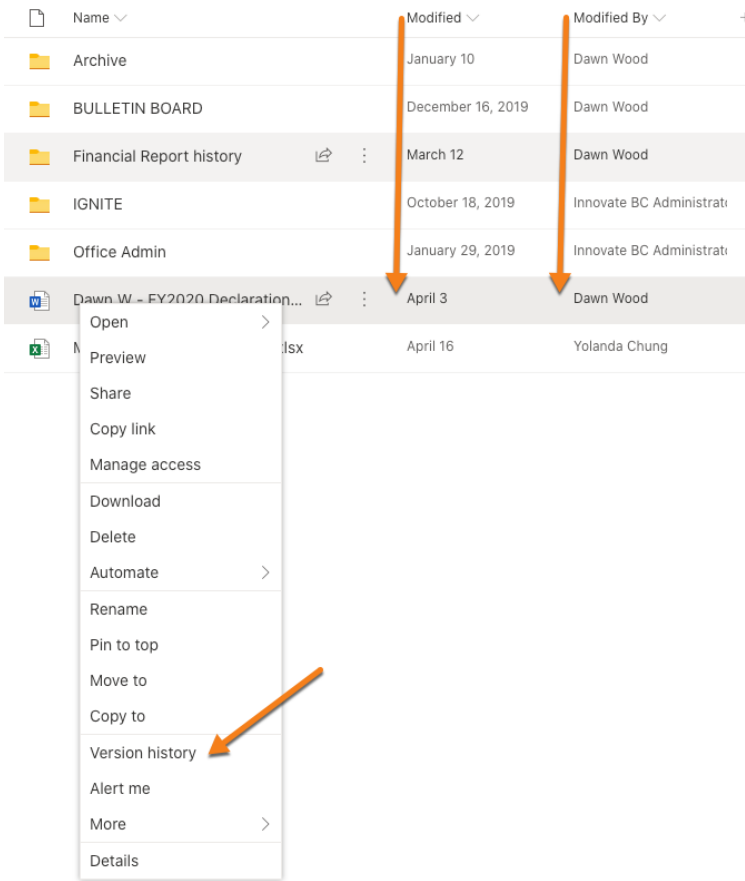
## 20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past.

Insert your own strategies if needed.

<b>Strategy</b>		
We only allow employees in certain roles access to information		
Employees that need standing or recurring access to personal information must be approved by executive lead		
We use audit logs to see who accesses a file and when		
<b>Describe any additional controls:</b>	<p><i>(IBC Note to user: the following text can be used here for data stored on Innovate BC server. This reply was provided by FullTech May 2020)</i></p> <p>Innovate BC uses Microsoft OneDrive &amp; SharePoint to store and server Office files. OneDrive &amp; SharePoint does have a mechanism to ascertain who modified which document and when as well as view and restore previous versions. We can also dig into backend logs to trace the lifecycle of any file. See the screenshot below:</p>	



Strategy																										
	 <table border="1"> <thead> <tr> <th>Name</th> <th>Modified</th> <th>Modified By</th> </tr> </thead> <tbody> <tr> <td>Archive</td> <td>January 10</td> <td>Dawn Wood</td> </tr> <tr> <td>BULLETIN BOARD</td> <td>December 16, 2019</td> <td>Dawn Wood</td> </tr> <tr> <td>Financial Report history</td> <td>March 12</td> <td>Dawn Wood</td> </tr> <tr> <td>IGNITE</td> <td>October 18, 2019</td> <td>Innovate BC Administrati</td> </tr> <tr> <td>Office Admin</td> <td>January 29, 2019</td> <td>Innovate BC Administrati</td> </tr> <tr> <td>Dawn.W. - FY2020 Declaration...</td> <td>April 3</td> <td>Dawn Wood</td> </tr> <tr> <td>M...lsx</td> <td>April 16</td> <td>Yolanda Chung</td> </tr> </tbody> </table>		Name	Modified	Modified By	Archive	January 10	Dawn Wood	BULLETIN BOARD	December 16, 2019	Dawn Wood	Financial Report history	March 12	Dawn Wood	IGNITE	October 18, 2019	Innovate BC Administrati	Office Admin	January 29, 2019	Innovate BC Administrati	Dawn.W. - FY2020 Declaration...	April 3	Dawn Wood	M...lsx	April 16	Yolanda Chung
Name	Modified	Modified By																								
Archive	January 10	Dawn Wood																								
BULLETIN BOARD	December 16, 2019	Dawn Wood																								
Financial Report history	March 12	Dawn Wood																								
IGNITE	October 18, 2019	Innovate BC Administrati																								
Office Admin	January 29, 2019	Innovate BC Administrati																								
Dawn.W. - FY2020 Declaration...	April 3	Dawn Wood																								
M...lsx	April 16	Yolanda Chung																								

## PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

### 21. How will you make sure that the personal information is accurate and complete?

[FOIPPA section 28](#) states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

### 22. Requests for correction

[FOIPPA](#) gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

**(IBC Note: be aware when responding to this question that FOIPPA legislation requires that public bodies allow individuals to request that their personal information be corrected)**

**22.1 Do you have a process in place to correct personal information?**

Type “yes” or “no” to indicate your response.

**22.2 Sometimes it’s not possible to correct the personal information. [FOIPPA](#) requires that you make a note on the record about the request for correction if you’re not able to correct the record itself. Will you document the request to correct or annotate the record?**

Type “yes” or “no” to indicate your response.

**22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, [FOIPPA](#) requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?**

Type “yes” or “no” to indicate your response.

**23. Does your initiative use personal information to make decisions that directly affect an individual?**

Type “yes” or “no” to indicate your response.

- If yes, go to [question 24](#)
- If no, skip ahead to [Part 7](#)

**24. Do you have an information schedule in place related to personal information used to make a decision?**

[FOIPPA](#) requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Type “yes” or “no” to indicate your response.

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

## PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

### 25. Will your initiative result in a personal information bank?

Type “yes” or “no” to indicate your response.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

## PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

### 26. Risk response

**Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.**

Add new rows if necessary.

Possible risk	Response
<i>Risk 1:</i> (IBC Note to user: include this row, provided by FullTech May 2020)  Data on the server is manipulated or accessed erroneously either by accident or with malice	??
<i>Risk 2:</i> (IBC Note to user: include this row, provided by FullTech May 2020)  Cloud is hacked	??
Risk 3:	
Risk 4:	

## PART 9: SIGNATURES

(IBC note that can be deleted after completing the form: We have been advised by Privacy Officer that IBC does not complete Part 9 – the OCIO would normally complete these parts. However, IBC is not required to have OCIO or any party sign off on our PIAs.)

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

### Privacy Office Comments

### Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
<b>Privacy Officer / Privacy Office Representative</b>			

### Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

### Program Area Comments:

Role	Name	Electronic signature	Date signed
<b>Initiative lead</b>			
<b>Program/Department Manager</b>			
<b>Contact Responsible for Systems Maintenance and/or Security</b> Only required if they have been involved in the PIA			
<b>Head of public body, or designate (if required)</b>			

# *Data Standardization Recommendations*



innovate **BC**



# Objectives

- Provide a recommended list of initial variables to be standardized across all Innovate BC programs.
- Create a list of proposed variable options for standardization across departments.
- Align variables with Statistics Canada and provincial datasets for future data sharing.



# Challenges Using Current Data

We've faced multiple challenges working with the current data available:

1. Data points are disjointed across multiple programs.
  - Each department (i.e.: Growth, Tech Adoption, Talent) determines its own data variables, guided by the key performance indicators that it must report.
  - Departments have similar variables but different options – becomes difficult to amalgamate the data and difficult to do a direct comparison across departments.
2. No standardized guide on which data should be available across programs.



# Standardization Can Help...

Standardizing data across programs will help remove some of the challenges we face:

- Will help reduce differences in data across departments
- Will help produce datasets that are analyzable, straightforward to report
- Will provide deeper, more holistic insights about companies and start-up growth trends
- Will allow us to integrate additional data from external sources



# Data Alignment

## 1. Statistics Canada

- Economic, social, and census data
- Aligning with Statistics Canada will allow Innovate BC to use Statistics Canada datasets for deeper analysis

## 2. Open Data Catalogues

- An open data initiative for data transparency. Independent of Statistics Canada data.
- Municipal/provincial/federal agencies publish data catalogues.

## 3. Other 3<sup>rd</sup> Party Organizations (e.g. ISED)

- Currently ISED data is not publicly available
- Uncertain if it aligns with Statistics Canada, but it's likely.



# Recommendations

1. Departments should work together to agree on a mutual set of questions/options that will be asked for participants.
  - The new questions should be implemented for the FY 2023 cycle.
2. Programs should set a deadline of June 30 for all final reporting.
  - The snapshot as of June 30 will be used for that year's impact report.





# Standardization Part 1 – Primary Variables

Working with program directors to identify critical variables to be standardized across all programs. Connected directly to key performance indicators for Innovate BC.

Recommended variables to standardize:

- Company Name
- Company HQ Street Address & Postal Code
  - City
  - Region
- Company Size
- Industry / Sector\*
- Company Stage
- Underrepresented demographics\*
- Organization Type



# Current State - Company Size

Current state of the company size breakdown:

ISI	DS4Y	Palette Skills	Emily Carr	Ignite	BC Fast	Challenges	VAP	ScaleUP	NVBC
			Does the Company	Patent Intentions: Does the consortium believe that protecting its Intellectual Property is a necessary					Does the company
Number of full-time	How many Full-Time Employees does the company employ?						Baseline Total Num	Baseline Total Number of Employees	
1-10	1-10								
11-20	11-20								
21-50	21-50								
51-99	51-99								
100-200	100-200								
201-300	201-300								
301-400	301-400								
401-500	401-500								
>500	>500								

VAP/Scale Up collect data on number of founders/entrepreneurs.



# Recommended State - Company Size

Recommended change for Company Size variable:

- **Question:** What is the size of your company?
- **Type:** Single-choice dropdown
- **Options:**
  - 0-4
  - 5-9
  - 10-19
  - 20-49
  - 50-99
  - 100-199
  - 200-299
  - 300-399
  - 400-499
  - 500+

*Data is aligned with Statistics Canada classifications.*



innovate BC

# Current State – Company Stage

Current state of the company stage breakdown:

ISI	DS4Y	Palette Skills	Ignite	BC Fast	Challenges	VAP	ScaleUP	NVBC
Company Stage	Company Stage		Company Stage		Stage of innovation at On-Set of Project	Venture Stage	Venture Stage	Company Stage
Startup - starting new business	Startup - starting new business		Startup					
Growth - increasing revenue	Growth - increasing revenue		Market Penetration/Growth					
Scale-up - scaling revenue	Scale-up - scaling revenue		Market Expansion/Scale					
Established								
						Product Validation	Product Validation	
						Market Validation	Market Validation	
						Market Penetration	Market Penetration	
						Market Expansion	Market Expansion	



# Recommended State - Company Stage

Recommended change for Company Stage variable:

- **Question:** What is the stage of your company?
- **Type:** Single-choice dropdown
- **Options:**
  - Startup – starting new business
  - Growth – increasing revenue
  - Scaling up – scaling revenue
  - Established company

*Data is not aligned with any external sources.*



innovate BC



# Current State – Company Sector

Current state of the company sector breakdown:

ISI	DS4Y	Palette Skills	Ignite	BC Fast	Challenges	VAP	ScaleUP	NVBC			
Employer Industry Sector	Company Sector		Company Sector	Industry Sector		Technology Industry	Technology Industry	Technology Sector			
Agriculture	Agriculture		Agriculture	Agriculture		Agriculture	Agriculture	Agriculture			
Advanced Materials	Advanced Materials & Advanced Manufacturing		Advanced Materials	Advanced Materials & Advanced Manufacturing		Advanced Materials	Advanced Materials	Advanced Materials & Advanced Manufacturing			
Clean Tech	Clean Tech		Clean Technology	Clean Tech		Clean Tech	Clean Tech	Clean Technologies			
				Construction							
Consumer Retail	Consumer Retail		Consumer Retail	Consumer Retail		Consumer Retail	Consumer Retail	Consumer Retail			
Digital Applications	Digital Applications & ICT		Digital Media and Communications	Digital Media & Telecommunications		Digital Media and Communications	Digital Media and Communications	Digital Media and Telecommunications			
						Digital Applications	Digital Applications	Content and Information and Communications Technology			
Education	Education		Education	Education		Education	Education	Education			
				Energy							
Financial Services	Financial Services		Financial Services	Financial Services		Financial Services	Financial Services	Financial Services			
Food & Beverage	Food & Beverage		Food & Beverage	Food & Beverage		Food & Beverage	Food & Beverage	Food & Beverage			
Forestry	Forestry		Forestry	Forestry		Forestry	Forestry	Forestry			
Life Sciences & Advanced Health	Life Sciences & Advanced Health		Life Sciences and Advanced Health	Life Sciences & Advanced Health		Life Sciences & Advanced Health	Life Sciences & Advanced Health	Life Sciences and Advanced Health			
				Manufacturing & Materials							
Mining, Oil & Gas	Mining, Oil & Gas		Mining, Oil & Gas	Mining, Oil & Gas		Mining, Oil & Gas	Mining, Oil & Gas	Mining, Oil & Gas			
Software & Computer Systems	Software & Computer Systems										
Tourism, Culture, Sports & Entertainment	Tourism, Culture, Sports & Entertainment		Tourism and Culture	Tourism and Culture		Tourism and Culture	Tourism and Culture	Tourism and Culture			
Transportation	Transportation		Transportation	Transportation		Transportation	Transportation	Transportation			
Other	Other		Other	Other		Other	Other	Other			



# Recommended State - Company Sector (1)

Recommended change for Company Sector variable:

- **Question 1:** Which best describes your company's industry sector?
- **Type:** Single-choice dropdown
- **Options:**
  - Agriculture, forestry, fishing and hunting
  - Mining, quarrying, and oil and gas extraction
  - Utilities
  - Construction
  - Manufacturing
  - Wholesale trade
  - Retail trade
  - Transportation and warehousing
  - Information and cultural industries
  - Finance and insurance
  - Real estate and rental and leasing
  - Real estate and rental and leasing
  - Professional, scientific and technical services
  - Management of companies and enterprises
  - Administrative and support, waste management and remediation services
  - Educational services
  - Health care and social assistance
  - Arts, entertainment and recreation
  - Accommodation and food services
  - Other services (except public administration)
  - Public administration

*Data is aligned with Statistics Canada NAICS classifications.*



innovate BC

# Recommended State - Company Sector (2)

Recommended change for Company Sector variable:

- **Question 2:** Is your company in any of the following additional sectors?
- **Type:** Single-choice dropdown
- **Options:**
  - Agriculture
  - Advanced Materials & Advanced Manufacturing
    - **Excludes** specifically forestry, agriculture, mining, clean technologies and life sciences
  - Clean Technologies
    - *Technologies that protect and/or increase efficient utilization of land, water and air resources.*
  - Consumer Retail
  - Digital Media and Telecommunications
    - *Digital applications and content and information and communications technologies.*
    - **Excludes** healthcare, agriculture, forestry, mining, financial services, education, social innovation, culture/recreation and energy-related solutions.
  - Education
  - Financial Services
  - Food & Beverage
  - Forestry
  - Life Sciences and Advanced Health
  - Mining, Oil & Gas
    - **Includes** extractive activities that would not otherwise fall under clean technologies.
  - Tourism and Culture
    - **Includes** entertainment and sports
  - Transportation
  - Other

*Data is aligned with ISED classifications.*



innovate BC

# Standardization Part 2 – Secondary Variables

The second stage will involve identifying additional variables of interest to be standardized across all programs. These variables are optional, program agnostic and can be used across multiple programs.

Recommended variables to standardize:

- Year of Company Incorporation
- Business Registration Number
- Company Description



# Standardization Part 3 – Economic Impact Indicators

Part 3 includes working with program directors to identify and organize departmental economic impact indicators.

Recommended variables to standardize:

- Customers acquired
- Revenue generated
- Investment generated
- Jobs created
- Jobs maintained / retained



# Questions...

1. How do we align our reporting timelines across departments to ensure that the most up-to-date data is collected, available, and reported?
  - BC Fast particularly - how do we align the program?
  - How do we align other ongoing programs?
  - How do align reporting from partners?
2. When do we “freeze” our datasets?
  - Which date do we use as a reporting date?
1. Privacy – how can we ask deeper DEI questions for better data while respecting privacy and FOIPPA?





**For:** CEO Innovate BC

**Issue:** Consolidation of transitory communications to Teams

**Date:** April 2<sup>nd</sup>, 2024.

**Background:**

- Innovate BC is a Crown agency that is listed under schedule B of the Freedom of Information and Protection of Privacy Act (FOIPPA). Under FOIPPA, IBC is required to comply with various requirements including properly managing transitory communications and retaining documents needed for effective records management.
- During the pandemic, IBC moved to a hybrid model of work and increasingly adopted various tools to facilitate virtual communications and decision making. These included Teams, Slack, Skype, email and other forms of instant communication.
- The array of platforms has led to increased costs, communication channel confusion and challenges ensuring that appropriate records are retained.

**Discussion:**

- Innovate BC management has agreed to consolidate communications platforms and will switching all transitory communications to Teams. As part of this shift, Slack and other channels will be decommissioned. To ensure effective management of transitory records, Teams will be set to only archive messages for a period of 30 days.
- To ensure records are properly managed, decisions and key policy, program and other direction will be managed through emails and use of information notes and decision notes. The latter will be centrally managed and filed out of the CEO's office.
- To support this transition, staff will receive information and training on proper document management and retention so there is awareness of compliance requirements and how to manage records. Completion of awareness training will also be included in annual performance plans and assessed.



---

Peter Cowan, President & CEO

**April 10, 2024**

---

Date

**Subject:** Re: Slack to Teams  
**Date:** Monday, April 29, 2024 at 4:37:40 PM Pacific Daylight Saving Time  
**From:** Michelle Foster  
**To:** Innovate BC Staff

Hey Team,

Quick update on the 30-day Teams retention policy.

We're ready to move ahead and Fulltech is going to push out the deletion policy to take place EOD **on Thursday, May 2<sup>nd</sup>**.

-  
If you have any important info you need to hold on to, please make it a priority to transfer and save that data prior to May 2<sup>nd</sup>.

Note: It can take Microsoft up to 7 days for the new retention policy to be applied, however, it's best to err on the side of caution and assume data will be lost after May 2<sup>nd</sup>.

Please let me know if you have any questions or concerns.

Thanks,  
Michelle

---

**From:** Michelle Foster <[mfoster@innovatebc.ca](mailto:mfoster@innovatebc.ca)>  
**Date:** Wednesday, April 10, 2024 at 2:01 PM  
**To:** Innovate BC Staff <[staff@innovatebc.ca](mailto:staff@innovatebc.ca)>  
**Subject:** Slack to Teams

Hey Team,

As discussed at last week's the staff meeting, we'll be switching up our internal communication platform from Slack to Microsoft Teams with a full implementation date targeted for the end of May. As of June, staff will be expected to move [transitory communications](#) to Microsoft Teams from Slack and other channels so we are compliant with *FOIPPA* and the *Information Management Act* which apply to our retention and provision of records. The shift to one platform will also help us save money and ensure that everyone is using one platform which will result in faster response times and fewer missed alerts.

Here's what you need to know:

1. **Keeping Slack for External Communication:** Don't worry, we're still keeping Slack around for chatting with our external partners. I'm aware of the BCAN Channel, and understand there may be a few more? If you could please let me know of any other external

partners you engage with before the transition date, by May 1<sup>st</sup>, ideally, that would be fantastic.

2. **30-Day Message Retention Policy:** With Teams, messages and chat history will only be retained for 30 days. So please remember not to drop any big decisions or super-important items there. Stick to email and decision notes for the important conversations and information that we are required to document and retain.
3. **Channel Transfer:** We'll be transferring over the main channels (9:09, Funstuff, General etc. ), along with the chat history. However, personal and department chats won't be transferred. So, if there's anything important in your personal/department chats, please save those conversations elsewhere prior to the transition date.

If you've got any questions or thoughts about this shift, please let me know.

Thanks,  
Michelle

**Michelle Foster** (she/her)  
Operations Manager

**Innovate BC**

**P:** 604-602-5221

**E:** [mfoster@innovatebc.ca](mailto:mfoster@innovatebc.ca)

1188 West Georgia St #900

Vancouver BC

**[Become an Innovate BC Insider](#)**

*Innovate BC's office is situated on the traditional and unceded territory of the x<sup>w</sup>məθk<sup>w</sup>əy əm (Musqueam), Skwxwú7mesh (Squamish), and səlilwətał (Tsleil-Waututh) Nations. We are grateful to work with innovators from across the traditional and unceded territories covering all regions of British Columbia.*



innovate BC

---

# Information Security Policy

Version 2.0 – Jan 2023



Table of Contents

Introduction .....1

Scope of this Policy .....1

Violations .....1

Communication Etiquette .....2

Personal Use .....2

Work Usage .....2

Document and Information Security.....3

Password and Access Codes .....3

Email .....4

Shared Files.....4

Copyrights and Licensing Agreements .....4

Ownership of Information and Access to Technology Records .....4

Freedom of Information and Protection of Privacy Act (FIPPA) .....5

Identifying and Avoiding Collection of Personal Information.....5

Database Contents and Access - Formal Approval Process .....5

Safeguarding Protected Information .....5

Privacy Impact Assessment(PIA).....6

Cloud-Based Applications .....6

Cloud Services Used by IT.....6

Payment/Credit Card Data .....8

Acceptable Use.....8

Mobile Phones .....8

Laptops .....8

Wireless .....8

Social Media .....10

Departures and Terminations.....10

Appendix A – Levels of Protected Information .....11

Appendix B – Protected Information Security Classification Levels .....12

Appendix C – Innovate BC Employee File Sharing Declaration .....13



## Introduction

The purpose of this policy and its associated procedures is to provide direction as to the acceptable uses of Innovate BC's information systems. The directives in this policy are intended to assist Innovate BC to:

- Protect its investment.
- Safeguard the information contained within its systems.
- Reduce business and legal risk.
- Protect the reputation of Innovate BC.

## Scope of this Policy

Access to and use of information systems at Innovate BC is provided to assist in the delivery of Innovate BC services. All use of computing and telecommunications facilities and equipment, including the Internet and e-mail, must comply with the requirements set out in this policy.

This policy pertains to all information systems used by Innovate BC or connecting to Innovate BC networks. Information systems include but are not limited to: personal computers, laptops, cloud applications, network or other storage media and mobile devices such as tablets and smart phones.

All full-time and part-time employees, contractors, volunteers and other individuals provided access to Innovate BC systems are covered by this policy. Throughout this policy, those who use computer systems will be referred to as 'end-users'.

This policy applies regardless of physical location.

## Violations

Violations may result in disciplinary action, which may extend to termination of employment or consulting contract.





### Communication Etiquette

Communications must be professional, factually correct and should not express personal opinions which are unrelated to a person's job duties.

Employees are expected to use Innovate BC's email system for business related communications. Personal e-mail accounts must not be used for Innovate BC business.

### Personal Use

Limited personal use of the internet by employees is allowable, provided it is consistent with professional conduct and does not violate the [acceptable use restrictions](#) listed on page 6.

Employees should exercise good judgment ensuring personal use does not interfere with Innovate BC's operations.

### Work Usage

Innovate BC users accessing the Internet are representing Innovate BC and are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Information transmitted on the Internet or stored on servers accessible via the Internet may be logged or viewed by unintended audiences. Internet usage must be consistent with the values of Innovate BC and the public's expectations of personal privacy.

Users must not knowingly attempt to access web sites that might bring Innovate BC into disrepute, such as those that contain material that violates any of Innovate BC 's policies or contain pornography, hate literature, or any material that contravenes the BC Human Rights Act, Criminal Code or any other Federal or Provincial law.

Downloads of large and/or potentially copyrighted content such as application install files, movies, and music from the Internet for non-work related purposes is not permitted.

All Peer to Peer or file sharing web applications, such as uTorrent, are prohibited.

### Information Security Awareness & Training

Every Innovate BC user is responsible for participating in the protection of Innovate BC's systems, accounts, and data. Innovate BC will provide the user with tools, resources, and training to raise their awareness of current information security threats. Attendance of this training is mandatory.

Examples of such threats include, but are not limited to:

- Email phishing
- Fraudulent phone calls and text messages
- Fraudulent or compromised websites
- Malicious software or documents

If a user suspects that their account credentials or devices are at risk, it must be reported to their supervisor and Fulltech immediately.



### Email Phishing

Email phishing is an information security threat that uses social engineering in which an attacker sends an email that may:

- Impersonate Innovation BC systems or users,
- Impersonate another organization
- Request the user take a specific action (click a link, purchase gift cards)
- Make threats or demands (access will be cut off, package will not be delivered)
- Ask for sensitive information

Suspected phishing emails should be reported via the “Report Message” button in Outlook.

If a user is the victim of email phishing (clicks links, downloads files, provides information), it must be reported to their supervisor and Fulltech immediately.

### Attack and Phishing Simulation

Innovate BC may initiate a simulated attack on the systems and accounts under its control. The purpose of these simulations is to:

- Improve user information security awareness
- Create user familiarity with the reporting process.
- Confirm the effectiveness of new or existing security controls

Any such simulated attacks must have the express written permission of the <ROLE NAME HERE>.

Phishing simulation is a process where the goal is to safely expose Innovate BC users to examples of email phishing. The ideal outcome is for Innovate BC users to report the simulated phishing email.

Innovate BC may require additional training or controls for those users who are experiencing challenges with recognizing phishing emails, either simulated or real.

### Document and Information Security

All data must be stored in the appropriate location on Innovate BC's Office 365 shared document libraries to ensure that it is backed up and can be recovered in the event of a system failure, accidental deletion or data loss. Innovate BC files must not be stored on a user's home computer or laptop.

If a user suspects any improper access to files, it must be reported to their supervisor and Fulltech immediately.

### Password and Access Codes

Each user is responsible for the security and protection of their passwords. The recommended format for a stronger password is a combination of words with the addition of numbers and symbols to meet complexity requirements, e.g. Care 387 walk\$, dog2crazy fence brown! and Large-tan54 give. Users must not disclose passwords to others and must immediately change passwords if it is suspected that they have become known to others.

Employees must not use another person's password or account to access Innovate BC's systems, and must not gain, or attempt to gain, unauthorized access to any account on Innovate BC's systems.



### Email

It should be understood that e-mail sent outside of Innovate BC travels over the Internet and is not guaranteed to be private. Innovate BC has no control of email once it leaves its system and therefore cannot guarantee that an externally transmitted email message will be received.

### Shared Files

Innovate BC is legally required to protect personal information – we may not share or receive personal information without following the correct process. Also, Innovate BC does not share sensitive or confidential business information. If you are unsure or have any questions please contact the Director of Compliance + Governance.

File sharing outside the organization is not permitted unless you have written permission from a supervisor or director. Please complete the form found in [Appendix C here](#) and have it approved.

Once approved, you can send a link to an outside party in order that they may access and edit a file located on Innovate BC's cloud server. Links that you share will expire after 60 days.

### Remote Access

Attempting unauthorized access to Innovate BC's systems or attempting to breach any security measures on the systems is prohibited. Only remote access provisioned on your provided laptop may be used to connect.

It is the responsibility of each user with remote access privileges to ensure that their access is not used by unauthorized parties.

### Copyrights and Licensing Agreements

Users are legally bound to comply with all copyright acts and software license agreements. Users are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner.

Only software that is licensed to or owned by Innovate BC is to be installed on Innovate BC computers.

### Ownership of Information and Access to Technology Records

All computing and telecommunications activities generate records of use including the date, time and type of access. These records are generated regardless of whether the usage is business or personal.

All information stored or recorded on or through Innovate BC's computing and telecommunications facilities belongs to Innovate BC and may be accessed for regular business, security or audit purposes without notice to the user. Be aware certain information may have to be released to the public if it is requested under the Freedom of Information and Protection of Privacy Act (FIPPA).

Innovate BC may access a user's data or e-mail at any time without notice to the user in the event of a security incident or if Innovate BC believes in its sole judgment that it has a business need to do so. All communications, including text and images, can be disclosed to law enforcement or other third parties as permitted or required by law without prior notification to the individuals involved.



## Freedom of Information and Protection of Privacy Act (FIPPA)

The Freedom of Information and Protection of Privacy Act (FIPPA) of BC aims to make public bodies more accountable to the public and to protect personal privacy by giving the public a right of access to records, a right to request correction of personal information about themselves and a right to prevent the unauthorized collection, use or disclosure of personal information by public bodies, among other things. All use of Innovate BC's information systems, including cloud-based apps, must be consistent with the aims of FIPPA.

The complete FIPPA text can be found here

[http://www.bclaws.ca/Recon/document/ID/freeside/96165\\_00](http://www.bclaws.ca/Recon/document/ID/freeside/96165_00)

## Identifying and Avoiding Collection of Personal Information

Under the FIPPA, 'personal information' is defined as "recorded information about an identifiable individual other than business 'contact information'".

"Contact information" is the type of information that appears on a business card and is defined as "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."

Information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information".

When collecting information, be aware that anything not considered "contact information" should be identified as Protected Information and will require extra efforts to limit access, prevent copying and enable a process to allow access and correction by the client, the data owner.

**Limit collection of information as much as possible to "contact information" only, unless there is a specific business requirement.**

## Database Contents and Access - Formal Approval Process

Be aware that internal requests for data from databases or for access to databases could result in the transfer of Protected Information.

Requests for data or access to databases must be formally approved by the Manager responsible for the database. The Manager must identify whether the request will involve Protected Information and if so, must evaluate privacy impacts and security risks of the request and implement the appropriate precautions.

To help identify the sensitivity of Protected Information see [Appendix A – Levels of Protected Information](#) and [Appendix B – Protected Information Security Classification Levels](#) on pages 8 and 9.

## Safeguarding Protected Information

Should it become necessary to collect or store information identified as 'Protected Information', extra efforts should be taken to guard the information and its accuracy. These would include, but not be limited to:

1. Making sure permission has been gained from the individual to collect this information
2. Using access controls to limit visibility to only those who require access for business purposes
3. Having a process to allow people to request and correct such collected information
4. Using encryption when transmitting such information over email or the internet
5. Storage and transmission only within Canada, except when explicit permission has been obtained



These controls should have as their aim to reduce threats of unauthorized use or disclosure of confidential or personal information.

### Privacy Impact Assessment (PIA)

In order to determine the risk level of new initiatives being considered, the BC Provincial Government offers a tool called a Privacy Impact Assessment (PIA). Smaller government bodies such as Innovate BC can complete this as a self-assessment in order to assess risk. Completing a PIA can help you to determine if personal information is at risk of being collected.

PIA documents can be found at <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments>

A guideline to filling out a PIA can be found here [https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia\\_guidelines.pdf](https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf)

### Cloud-Based Applications

Cloud-based computing solutions have become increasingly attractive to business users due to their ease of use, availability and low cost, but they can involve significant information security risk. These services can also result in the storage, access and/or disclosure of personal information outside Canada, which is prohibited in the FIPPA, unless the individual has expressly been made aware of this and given permission.

#### FIPPA states

30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

(a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;

When collecting data using a service that may store data outside of Canada, be sure to clearly indicate this is the case, and have the user click to agree. Also, provide a link to the site's privacy and security policy.

### Cloud Services Used by IT

IT does use some US- based third-party cloud services that collect and store certain business-related information in order to provide troubleshooting or consulting advice. This can include your business contact information, including your personal cell-phone number if you use it for business as well as an encrypted version of your password.

These systems include:

#### Zendesk

Your personal and non-personal information may become recorded into our ticketing system called Zendesk. This information is used only for the purposes of contacting you to offer our technical support services. Please be aware that if you volunteer any additional personal information via the email [support@fulltech.ca](mailto:support@fulltech.ca), it will be stored in that conversation thread and remain on Zendesk servers.

#### Mosyle Business

Mosyle Business may be installed on your Innovate BC-owned computers.

The system does not track and record computer location data but does track and record any Innovate BC-owned and supplied iOS devices. For a full list of what data Mosyle collects, click here:

<https://business.mosyle.com/legal/privacy>

#### ITGlue

FullTech uses a service called ITGlue to remember passwords for your Office 365 license (Microsoft Office) plus company admin passwords for the I.T. infrastructure. This



information is encrypted and is only used by FullTech in the provision of its I.T. related services.





## Payment/Credit Card Data

Client credit card numbers should never be collected, transmitted or stored electronically on Innovate BC's systems (e.g. e-mail, messaging, network drive, etc)..

Should it be decided to take credit card payments in-house in the future, the Payment Card Industry provides a set of guidelines that can be reviewed for best-practices and risk mitigation. These can be found at <https://www.pcisecuritystandards.org/>. It is always best to use a reputable third party to process client credit card payments to avoid the risk of having any customer credit card information stored in-house.

It is OK to conduct an electronic transaction as the cardholder (individual identified on the credit card or authorized to use the credit card). Be cautious the site you are dealing with is reputable.

## Acceptable Use

Innovate BC is committed to maintaining a respectful workplace environment. Use of Innovate BC's information systems must not contravene any company policies. Users must not create, transmit, distribute, forward, download or store any software, documents, files or information that:

- ✗ infringes any copyright, trademark, trade secret, or other intellectual property right;
- ✗ is obscene or pornographic;
- ✗ is libelous, defamatory, hateful, or constitutes a threat or abuse;
- ✗ is or encourages conduct that would constitute a criminal or other offence or give rise to liability;
- ✗ harasses the receiver, whether through content, frequency, or size of message(s);
- ✗ is junk mail, spam, or chain e-mail;
- ✗ impersonates another person or misrepresents the sender's identity;
- ✗ exposes Innovate BC or its employees to unauthorized legal obligations or liability;
- ✗ divulges private and/or confidential information related to Innovate BC's business, clients and/or employees;
- ✗ could be deemed as offensive based on (but not limited to) race, gender, religious beliefs, age or sexual orientation.

## Mobile Phones

Personal phones are permitted to access Innovate BC's email systems.

Note that all Innovate BC email accessed via a personal phone remains the property of Innovate BC and is subject to this policy. Upon leaving employment with Innovate BC, the email connection will be terminated and Fulltech will wipe all Office 365 data on the ex-employee's device remotely.

## Laptops

Users are responsible for the custody of their laptop and mobile. In the event of a loss or suspected theft of a Innovate BC issued laptop or mobile device, it must be promptly reported to the Operations Manager and Fulltech.

All laptops that connect to Innovate BC's Office 365 OneDrive or SharePoint are required to use Multi-Factor Authentication (MFA). MFA is set up by Fulltech when a new employee joins Innovate BC. When a new employee first logs in to any Office 365 application, they will be prompted to set up MFA on their phone before they can access any Office 365 applications.

## Wireless

Users must not install their own wireless access points on Innovate BC's sites.





## Social Media

Public bodies can use social media for purposes such as:

- ✓ Providing useful information to citizens;
- ✓ Facilitating a forum for citizen engagement and discussion;
- ✓ Promoting existing initiatives or policies;
- ✓ Posting public photos of events;
- ✓ Notifying users of further opportunities for discussion; or
- ✓ Updating users on the progress of a matter under discussion.

Avoid soliciting or collecting personal information.

Forums should be moderated to remove any unsolicited comments or information about anyone other than the person posting. A contact name should be provided for any questions. Any unmoderated or inactive social media accounts should be deleted.

Care should be taken that any online communications do not adversely impact or create issues for Innovate BC, its employees, or its clients. It is difficult to delete content and impossible to remove all traces of its existence even when deleted once it is posted to a site, so caution is needed when writing any posting.

When using Innovate BC's social media channels, you are personally responsible for all content you post online. Use discretion and judgement in sharing information to ensure that Innovate BC's confidentiality and harassment policies are not contravened, and/or that information shared could in any way damage Innovate BC's reputation or image.

Unless authorized by Innovate BC in writing, when using Online Communications, you are specifically prohibited from:

- ✗ Disclosing proprietary, non-public Innovate BC information.
- ✗ Divulging confidential information of any person or company affiliated with Innovate BC.
- ✗ Posting any private photographs of individuals unless you have obtained prior written consent
- ✗ Sending or posting messages that disparage another organization's products or services.

If you discover, or are informed of any Innovate BC related comments on social media sites and you believe these comments should be addressed, contact Innovate BC's Director, Marketing & Communications for advice.

## Departures and Terminations

The Operations Manager should be notified promptly whenever an employee is hired, leaves the company or changes job titles so that network access can be created, modified or revoked in an expedient manner. Involuntary terminations must be reported concurrent with the termination. Upon departure or termination, all employee system access will be disabled. Any company equipment in the employee's possession must be returned.

E-mail and personal files can be transferred to a new user as required. An e-mail rule will be created to auto-respond with new contact information.

User network and e-mail accounts may be maintained after the employee has left, but will be assessed every 4 months to see if it is necessary to keep the account active or if it can be archived or deleted.

All files and information must be archived from any hard drives or removable media that is being transferred to a new user or disposed of. After archiving, old hard drives may still contain residual data even after reformatting, so should not be reused externally. Requests for secure data deletion should be submitted to the Operations Manager.

Appendix A – Levels of Protected Information

Sensitivity	Definition	Illustrative Examples	Labels
HIGH	<p>Could possibly be expected to cause extremely serious personal or enterprise injury, including any combination of:</p> <p>Financial harm, such as:</p> <ul style="list-style-type: none"><li>a. Extremely significant loss of money or tangible assets</li><li>b. Extremely significant penalties or recovery costs incurred</li></ul> <p>Operational harm, such as:</p> <ul style="list-style-type: none"><li>a. Severely impaired decision making, resulting in severe loss of program control</li><li>b. Program closure or serious sanctions as a result of breach of legislation, contract or regulatory standards</li><li>c. Major political impact - complete and extended loss of public trust or confidence in government</li></ul> <p>Personal harm, such as:</p> <ul style="list-style-type: none"><li>a. Loss of life</li><li>b. Extreme hazard to public safety</li><li>c. Wide spread social hardship</li></ul>	<ul style="list-style-type: none"><li>• Personal information combined with any highly sensitive information.</li><li>• Cabinet documents.</li><li>• Extremely confidential information and information that is intended for access by named individuals or positions only.</li><li>• Justice sector confidential information (e.g., law enforcement information, court information, witness protection programs).</li><li>• Provincial budget prior to public release.</li><li>• Crisis communication during emergencies and provincial response plan and logs.</li><li>• Emergency information (e.g., pandemic, natural disasters).</li><li>• Information systems used for testing food or water supplies that could result in loss of life or severe illness.</li><li>• Extremely large financial transactions (e.g., over \$1 million).</li></ul>	<ul style="list-style-type: none"><li>• High Sensitivity</li><li>• Cabinet Confidential</li></ul>
MEDIUM	<p>Could possibly be expected to cause serious personal or enterprise injury, including any combination of:</p> <p>Financial harm, such as:</p> <ul style="list-style-type: none"><li>a. Significant financial loss, penalty, or recovery expense</li></ul> <p>Operational harm, such as:</p> <ul style="list-style-type: none"><li>a. Significant impact on service levels</li><li>b. Serious loss of confidence in a government program</li><li>c. Damage to partnerships, relationships and reputation</li><li>d. Staff forced to resign</li></ul> <p>Personal harm, such as:</p> <ul style="list-style-type: none"><li>a. Serious personal hardship or embarrassment</li></ul>	<ul style="list-style-type: none"><li>• Sensitive personal information (personal medical or health information, tax information, information describing personal finances, eligibility information for social benefits).</li><li>• Information intended for a specific group only.</li><li>• Trade secrets or intellectual property.</li><li>• Business or other third party information.</li><li>• Provincial standardized tests for schools.</li><li>• Information relating to minors (e.g., adoption and foster records, medical and forensic psychiatric services).</li><li>• Information on young offenders.</li><li>• Citizen payments of benefits (e.g., BC Benefits, Disability Benefits, Guaranteed Available Income for Need).</li><li>• Business Continuity Plan information.</li><li>• Identity information that could be used for criminal purposes (e.g., from Vital Stats, ICBC).</li><li>• Information on investigations and active incidents.</li><li>• Law enforcement records.</li><li>• Employee personnel files and work history data.</li><li>• Information systems that must not be unavailable beyond 1 business day.</li><li>• Financial management information systems (e.g., payroll, payments, accounts receivables, over</li></ul>	<ul style="list-style-type: none"><li>• Medium Sensitivity</li><li>• Personal*</li></ul> <p>* Personal label is used for information that identifies a person and its disclosure may cause a serious harm to the person. When the "personal" information is combined with higher sensitive information, it should be classified as "High".</p>
LOW	<p>Could reasonably be expected to cause limited or no injury to individuals or enterprises, including any combination of:</p> <p>Financial harm, such as:</p> <ul style="list-style-type: none"><li>a. Limited financial loss</li></ul> <p>Operational harm, such as:</p> <ul style="list-style-type: none"><li>a. Limited impact on service levels</li><li>b. Reduced staff effectiveness due to loss of morale</li></ul> <p>Personal harm, such as:</p> <ul style="list-style-type: none"><li>a. Minor embarrassment or inconvenience</li></ul>	<ul style="list-style-type: none"><li>• Pre-approved personal information for release.</li><li>• Information that is generally available to employees and approved non-employees (e.g., contractors, vendors, service providers, or consultants).</li><li>• Non-sensitive information, suitable to release.</li><li>• Ordinary meeting agendas and minutes.</li><li>• Communications to claims clerks.</li><li>• Job applicants' names.</li><li>• External press releases, media/public distribution.</li><li>• Operational procedures related to non-critical activities.</li><li>• Provincial budget after public release.</li><li>• Public accounts after publication.</li><li>• Public education materials.</li><li>• Information systems that can be down for up to 3 days.</li><li>• Financial transactions (e.g., under \$100,000).</li><li>• Information published by government, which</li></ul>	<ul style="list-style-type: none"><li>• Low Sensitivity</li><li>• Public</li></ul>

Appendix B – Protected Information Security Classification Levels

	Level	Description
	Public	No harm to an individual, organization or government Examples: Job postings, communications to claim clerks, business contact information, research and background papers
Confidential	Protected A	Harm to an individual, organization or government Examples: Home addresses, dates of birth, other low-risk personal
	Protected B	Serious harm to an individual, organization or government Examples: Law enforcement and medical records, personnel evaluations and investigations, financial records, information subject to solicitor-client privilege or other legal privilege
	Protected C	Extremely grave harm to an individual, organization or government Examples: Information about police agents and other informants, Cabinet records or Cabinet-related records

See original [here](#)



Appendix C – Innovate BC Employee File Sharing Declaration

You have been assigned file sharing rights, which means that you can send a link to an outside party in order that they may access and edit a file located on Innovate BC’s cloud server. Links that you share will expire after 60 days.

Innovate BC is legally required to protect personal information – we may not share or receive personal information without following the correct process. Also, Innovate BC does not share sensitive or confidential business information.

To avoid the above, please consider whether any of the information in your file is:

- Personal – non-professional information that can be used to identify a person. For example:
  - A name (e.g. a student, an event attendee)
  - Personal email address
  - Personal phone number
  - Home address
  - Gender
  - Race
  - Opinions about the individual or their opinions
- Sensitive or confidential business information examples:
  - Intellectual Property
  - Budgets
  - information on risks to business
  - plans to commercialize,
  - Investment or revenue numbers
  - Funding proposals may often contain the above

If you identify that the file you wish to share includes personal or sensitive or confidential business information, do not share the documents and ask for advice.

I have read the above information and understand my obligation as an Employee of Innovate BC to avoid sharing or receiving protected information with or from outside parties.

\_\_\_\_\_  
Name (Print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor Signature

October 21, 2024

Spencer Izen  
Legal & Social Science Researcher  
B.C. Freedom of Information and Privacy Association

**Subject: FIPA FOI 371 Request dated August 21, 2024**

Dear Spencer,

Thank you for the inquiry and granted extension. We are responding to your FOIPPA request dated August 21, 2024 regarding records from January 1, 2021 through to August 21, 2024. Please find below our response.

As a BC Crown Agency, Innovate BC relies on established policies and procedures by the provincial government as they relate to FOIPPA and the Information Management Act. We do not develop separate policies.

**1. Documenting government decisions” policy instruments (where “instrument” has the same meaning as in TBD 1/23)**

Responsive record include:

- 1. Memo on transitory records

**2. Final Requests for Proposals concerning records management/freedom of information (not privacy)**

We do not have responsive records as requested.

**3. Copies of checklists, forms, templates, guides and other tools used in relation to processing freedom of information requests**

Responsive records include:

- 2. IBC and FOIPPA 2021 Presentation Overview
- 3. New PIA Template 2023

**4. Contracts and statements of work for consultant services for freedom of information/records management work**

We do not have responsive records as requested.



**5. 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**

We do not have responsive records as requested.

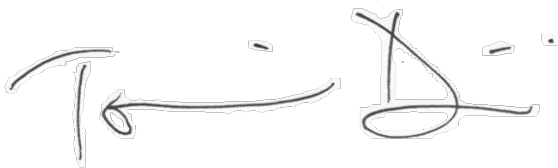
**6. Copies of any plans or assessments done in preparation for the application of the *Information Management Act* (e.g. Readiness Assessments for the provision relating to document government decisions)**

We do not have responsive records as requested.

**7. Any previously unrequested/undisclosed records that can 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.)**

We do not have responsive records as requested.

Best regards,



Tomica Divic

Vice President, Strategic Partnerships and Ecosystem Development

**For:** CEO Innovate BC

**Issue:** Consolidation of transitory communications to Teams

**Date:** April 2<sup>nd</sup>, 2024.

**Background:**

- Innovate BC is a Crown agency that is listed under schedule B of the Freedom of Information and Protection of Privacy Act (FOIPPA). Under FOIPPA, IBC is required to comply with various requirements including properly managing transitory communications and retaining documents needed for effective records management.
- During the pandemic, IBC moved to a hybrid model of work and increasingly adopted various tools to facilitate virtual communications and decision making. These included Teams, Slack, Skype, email and other forms of instant communication.
- The array of platforms has led to increased costs, communication channel confusion and challenges ensuring that appropriate records are retained.

**Discussion:**

- Innovate BC management has agreed to consolidate communications platforms and will switching all transitory communications to Teams. As part of this shift, Slack and other channels will be decommissioned. To ensure effective management of transitory records, Teams will be set to only archive messages for a period of 30 days.
- To ensure records are properly managed, decisions and key policy, program and other direction will be managed through emails and use of information notes and decision notes. The latter will be centrally managed and filed out of the CEO's office.
- To support this transition, staff will receive information and training on proper document management and retention so there is awareness of compliance requirements and how to manage records. Completion of awareness training will also be included in annual performance plans and assessed.

---

Peter Cowan, President & CEO

---

Date



# Protection of Privacy

Overview for the Innovate BC team

## Purpose

To provide team with the basic points to help you handle personal information while delivering Innovate BC activities.

There is no longer a single point person for all FOIPPA items.

Director of Marketing will oversee PIAS.

Jennie will delegate other items as they arise.



# This presentation will tell you:

- Definition of personal information
- When and how we may collect, use and share personal information
- Requirements of collecting and holding personal information



- Crown Agency of the Province of BC.
- A public body
- Subject to the Freedom of Information and Protection of Privacy Act (FOIPPA)

# Privacy Legislation

- There is legislation for public bodies and legislation for non-public orgs (eg businesses).
- There is federal legislation.
- Additionally, each province has their own privacy legislation which may be different from one another
- BC's laws for public bodies is called FOIPPA (PIPA for businesses etc)



# Definition of Personal Information

FOIPPA:

Simply put, personal information is any **recorded** information about an identifiable individual other than their business contact information. Personal information includes information that can be used to identify an individual through association or inference.

# Examples of Personal Information

- Name, age, sex
- Home address and phone number
- Race, ethnic origin, sexual orientation
- Number or symbol assigned to the individual
- Education
- Financial information
- Employment information
- Personal views or opinions, except if they are about someone else

## When we can collect personal information

A public body may only collect personal information if it has legal authority to collect it, if the information is for law enforcement purposes or if it is necessary for one of the public body's operating programs.

IBC team: for our use, it is usually 26c or 26e of FOIPPA that applies to our collection of personal information

## FOIPPA Section 26

- A public body may collect personal information only if:
- ...
- (c) the information relates directly to and is necessary for a program or activity of the public body,
- ...
- (e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

## How we may use personal information

A public body may generally only use personal information for the purpose it was collected, for a consistent purpose or with the individual's consent for another purpose.



## How we may share personal information

A public body may only disclose personal information for the purpose it was collected, for a consistent purpose, with the individual's consent or for one of the other specified purposes in the Act, such as law enforcement or to protect individual or public health or safety.

## If we collect personal information we must

- Store data in Canada
- Collect the data directly from the individual
- Post a collection notice
- Complete a Privacy Impact Assessment (PIA)
- Arrange for security of the information
- Strive for accuracy and completeness



## If we collect personal information we must

- Store data in Canada
- If we cannot or prefer not to store data in Canada (eg MailChimp, HubSpot),
  - consider the sensitivity of the information.
  - Obtain consent to store outside of Canada (in collection notice)

## If we collect personal information we must

- Collect the data directly from the individual
  - If we cannot, we must obtain written consent from the individual which authorizes the 3<sup>rd</sup> party to provide that information to us. The consent must tell the individual Innovate BC's purpose for collecting it. (eg DS4Y, VAP)

## If we collect personal information we must

- Post a collection notice
  - The collection notice should be apparent and viewable before the individual submits the information
  - At minimum the collection notice must tell the individual the purpose for collecting their personal information, the legal authorization under FOIPPA for collecting it and provide the business title, address and telephone number of an employee who can answer their questions about the collection.

# If we collect personal information, we must

- Complete a PIA
  - PIAs are a risk mitigation tool. They should be completed before an activity begins. PIAs help us think through the process to ensure we follow the correct steps.
  - Innovate BC PIAs are filed in Operations. You can ask Dir. Mktg for the template and send the completed PIA to Dir. Mktg.
  - PIAs must be kept up to date as program processes change. Most PIAs can be reviewed annually to check for necessary updates.

# If we collect personal information, we must

- Complete a PIA (continued)
  - Examples of PIAs for Innovate BC:
    - Event registration (the process and SaaS tools)
    - Newsletter/mailling list registration
    - Funding programs and related SaaS tools
    - Website
    - Scheduling tools
    - HR records
    - Event tools (eg Zoom)



## If we collect personal information, we must

- Arrange for security of the information
  - Consider the sensitivity of the information, **risk** of unauthorized access, use or disclosure and **effect on the individual** should unauthorized access, use or disclosure occur.
  - Take steps to secure the information accordingly.

## If we collect personal information, we must

- Strive for accuracy and completeness
  - A public body may correct an individual's personal information if the individual requests it and must make a note beside it showing the correction the individual requested



# Freedom of Information

# Freedom of Information Requests

FOI requests are managed by Jennie or Director of Marketing

FOI requests may be made by anyone in the public. For example, media makes requests of public bodies for all sorts of topics, such as approved expenses.

Written records of a public body are subject to an FOI request, including emails, slack threads, Teams chats, even text messages on your personal phone if the texts related to the topic of the FOI request.

These records will become public if they are related to the topic of an FOI request.

It is good practice to maintain professional standards in all messages including internal chats.



## FOIPPA Resources

- Director of Marketing
- Jennie (who may delegate to others)
- Online FOIPPA information
- Privacy Helpline (email and phone) – should be one point person for IBC that contacts Privacy Branch in most cases





# Privacy Impact Assessment for Non-Ministry Public Bodies

## Table of Contents

<b>Before you start</b> .....	1
<b>PART 1: GENERAL INFORMATION</b> .....	2
<b>PART 2: COLLECTION, USE AND DISCLOSURE</b> .....	4
<b>PART 3: STORING PERSONAL INFORMATION</b> .....	6
<b>PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA</b> .....	7
<b>PART 5: SECURITY OF PERSONAL INFORMATION</b> .....	10
<b>PART 6: ACCURACY, CORRECTION AND RETENTION</b> .....	13
<b>PART 7: PERSONAL INFORMATION BANKS</b> .....	15
<b>PART 8: ADDITIONAL RISKS</b> .....	15
<b>PART 9: SIGNATURES</b> .....	16

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in B.C. and are starting a new initiative or significantly changing an existing initiative.

## Before you start

- If you are in a non-ministry public body, you may use this template to document a PIA. This template leads you through a complete PIA, but you are welcome to use another template or method for documenting your PIA
- An initiative is an enactment, system, project, program or activity
- Find information on the [PIA review process](#) and [question-by-question guidance](#)



- If you have any questions, email [Privacy.Helpline@gov.bc.ca](mailto:Privacy.Helpline@gov.bc.ca) or phone [250 356-1851](tel:250-356-1851)

## PART 1: GENERAL INFORMATION

PIA file number:

<b>Initiative title:</b>	
<b>Organization:</b>	
<b>Branch or unit:</b>	
<b>Your name and title:</b>	
<b>Your work phone:</b>	
<b>Your email:</b>	
<b>Initiative Lead name and title:</b>	
<b>Initiative Lead phone:</b>	
<b>Initiative Lead email:</b>	
<b>Privacy Officer:</b>	
<b>Privacy Officer phone:</b>	
<b>Privacy Officer email:</b>	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the [Office of the Information and Privacy Commissioner](#).

(IBC Note that can be deleted after filling out the form: in IBC's case if we deliver it on our own, the answer to this will always be "no" because— IBC is one body. We are considered as part of the Ministry for the purpose of FOIPPA as a service provider.)



Yes/No
Is this initiative a common or integrated program or activity? Under section <a href="#">FOIPPA 69 (5.4)</a> , you must submit this PIA to the Office of the Information and Privacy Commissioner.
(IBC Note that can be deleted after filling out the form: Privacy Officer advised Dawn in the past that most cases are not in this category – if in doubt, check with Privacy Officer)
Yes/No
Related PIAs, if any:
List

### 1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

### 2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

### 3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

### 3.1 Did you list personal information in question 3?

**Personal information** is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Type “yes” or “no” to indicate your response.

- If yes, go to [Part 2](#)
- If no, answer [question 4](#) and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

### 4. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

## PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

### 5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
	Data team to complete this column	Data team to complete this column	Data team to complete this column
Step 1:			
Step 2:			
Step 3:			
Step 4:			

**Optional:** Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

## 6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Review the [sample collection notice](#) and write your collection notice below. You can also attach the notice as an appendix.

**IBC Note that can be deleted after completing this form:**

**FOIPPA legislation requires that public bodies include a “collection notice” whenever we collect personal information and it must include the items listed below.**

**Example notification for collection:**

This information is collected by Innovate BC under [section ??] of the Freedom of Information and Protection of Privacy Act (FOIPPA) and will be used to [purpose]. Should you have any questions about the collection of this personal information please contact

Director, Data + Policy

900 – 1188 West Georgia St

Vancouver, BC V6E 4A2

604-602-5238

## PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

*(IBC Notes to Innovate BC Staff. Please delete after completing the PIA)*

- *FOIPPA legislation requires that public bodies store personal information in Canada. If we must store personal information on servers outside of Canada we must get consent in the correct manner from the individual*
- *The following reply can be used for data stored on Innovate BC server (Question 8 below). This reply was provided by FullTech May 2020):*

Information and data is stored on a cloud server provided by Microsoft, located within Canada. Information can only be accessed outside of Canada by staff should they be travelling for example. Access outside of Canada by employees while travelling is authorized by FOIPPA section 33.1(1)(e).

### 7. Is any personal information stored outside of Canada?

Type "yes" or "no" to indicate your response.

### 8. Where are you storing the personal information involved in your initiative?

### 9. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response.

- If yes, go to [question 10](#)
- If no, go to [Part 5](#)

**10. Is the sensitive personal information being disclosed outside of Canada under [FOIPPA section 33\(2\)\(f\)](#)?**

Type “yes” or “no” to indicate your response.

- If yes, go to [Part 5](#)
- If no, go to [Part 4](#)

## **PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA**

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization’s Privacy Officer. More help is available in the [Guidance on Disclosures Outside of Canada](#).

**11. Is the sensitive personal information stored by a service provider?**

Type “yes” or “no” to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to [question 13](#)
- If no, go to [question 12](#)

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

**12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.**

**13. Does the contract you rely on include privacy-related terms?**

Type “yes” or “no” to indicate your response.

- If yes, describe the contractual measures related to your initiative.

**15. What controls are in place to prevent unauthorized access to sensitive personal information?**

**16. Provide details about how you will track access to sensitive personal information.**



**17. Describe the privacy risks for disclosure outside of Canada.**

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

### Outcome of Part 4

The outcome of Part 4 will be a **risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

## PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

### 18. Does your initiative involve digital tools, databases or information systems?

Type “yes” or “no” to indicate your response.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of [FOIPPA section 30](#)

#### 18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of [FOIPPA section 30](#)?

Type “yes” or “no” to indicate your response.

- If yes, you may want to append the security assessment to this PIA. Go to [question 20](#)
- If no, go to [question 19](#)

**19. What technical and physical security do you have in place to protect personal information?**

Describe where the digital records for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, you may want to append it to the PIA.

*(IBC Note to user on Physical Security measures: some examples you may wish to include in addition to any others you think of:*

*Information and Data for this program are stored on the cloud, not in physical media.*

*Access to the office requires a door code or key card.*

*Staff log out and physically secure their devices when not in use.)*

*(IBC Note to user on Technical Security measures: the following reply can be used for data stored on Innovate BC server. This reply was provided by FullTech May 2020)*

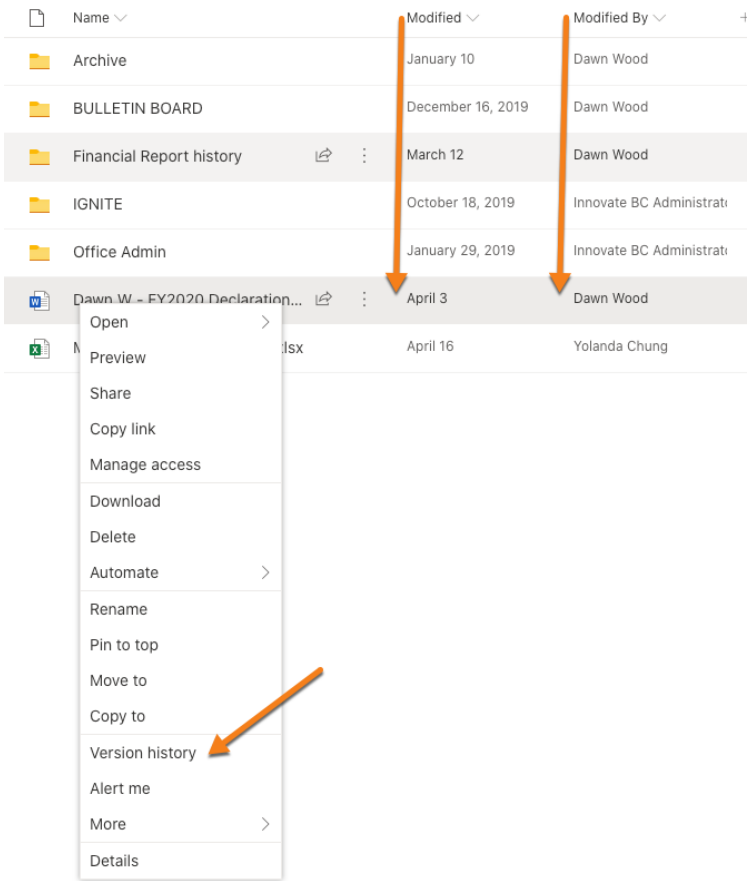
Innovate BC makes use of a modern firewall, endpoint full disk encryption, and user access accounts are assigned on a need-to-know basis. Innovate BC computers are configured with Mobile Device Management (MDM) that allows for remote lock, data wipe and security compliance enforcement. The Wi-Fi network at Innovate BC is configured with RADIUS to ensure only authorized personnel can access Innovate BC resources and data.

**20. Controlling and tracking access**

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past.

Insert your own strategies if needed.

<b>Strategy</b>		
We only allow employees in certain roles access to information		
Employees that need standing or recurring access to personal information must be approved by executive lead		
We use audit logs to see who accesses a file and when		
<b>Describe any additional controls:</b>	<p><i>(IBC Note to user: the following text can be used here for data stored on Innovate BC server. This reply was provided by FullTech May 2020)</i></p> <p>Innovate BC uses Microsoft OneDrive &amp; SharePoint to store and server Office files. OneDrive &amp; SharePoint does have a mechanism to ascertain who modified which document and when as well as view and restore previous versions. We can also dig into backend logs to trace the lifecycle of any file. See the screenshot below:</p>	

Strategy																										
	 <table border="1"> <thead> <tr> <th>Name</th> <th>Modified</th> <th>Modified By</th> </tr> </thead> <tbody> <tr> <td>Archive</td> <td>January 10</td> <td>Dawn Wood</td> </tr> <tr> <td>BULLETIN BOARD</td> <td>December 16, 2019</td> <td>Dawn Wood</td> </tr> <tr> <td>Financial Report history</td> <td>March 12</td> <td>Dawn Wood</td> </tr> <tr> <td>IGNITE</td> <td>October 18, 2019</td> <td>Innovate BC Administrati</td> </tr> <tr> <td>Office Admin</td> <td>January 29, 2019</td> <td>Innovate BC Administrati</td> </tr> <tr> <td>Dawn.W. - FY2020 Declaration...</td> <td>April 3</td> <td>Dawn Wood</td> </tr> <tr> <td>M...</td> <td>April 16</td> <td>Yolanda Chung</td> </tr> </tbody> </table>		Name	Modified	Modified By	Archive	January 10	Dawn Wood	BULLETIN BOARD	December 16, 2019	Dawn Wood	Financial Report history	March 12	Dawn Wood	IGNITE	October 18, 2019	Innovate BC Administrati	Office Admin	January 29, 2019	Innovate BC Administrati	Dawn.W. - FY2020 Declaration...	April 3	Dawn Wood	M...	April 16	Yolanda Chung
Name	Modified	Modified By																								
Archive	January 10	Dawn Wood																								
BULLETIN BOARD	December 16, 2019	Dawn Wood																								
Financial Report history	March 12	Dawn Wood																								
IGNITE	October 18, 2019	Innovate BC Administrati																								
Office Admin	January 29, 2019	Innovate BC Administrati																								
Dawn.W. - FY2020 Declaration...	April 3	Dawn Wood																								
M...	April 16	Yolanda Chung																								

## PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

### 21. How will you make sure that the personal information is accurate and complete?

[FOIPPA section 28](#) states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

### 22. Requests for correction

[FOIPPA](#) gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

**(IBC Note: be aware when responding to this question that FOIPPA legislation requires that public bodies allow individuals to request that their personal information be corrected)**

**22.1 Do you have a process in place to correct personal information?**

Type “yes” or “no” to indicate your response.

**22.2 Sometimes it’s not possible to correct the personal information. [FOIPPA](#) requires that you make a note on the record about the request for correction if you’re not able to correct the record itself. Will you document the request to correct or annotate the record?**

Type “yes” or “no” to indicate your response.

**22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, [FOIPPA](#) requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?**

Type “yes” or “no” to indicate your response.

**23. Does your initiative use personal information to make decisions that directly affect an individual?**

Type “yes” or “no” to indicate your response.

- If yes, go to [question 24](#)
- If no, skip ahead to [Part 7](#)

**24. Do you have an information schedule in place related to personal information used to make a decision?**

[FOIPPA](#) requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Type “yes” or “no” to indicate your response.



- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

## PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

### 25. Will your initiative result in a personal information bank?

Type “yes” or “no” to indicate your response.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

## PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

### 26. Risk response

**Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.**

Add new rows if necessary.

Possible risk	Response
<i>Risk 1:</i> (IBC Note to user: include this row, provided by FullTech May 2020)  Data on the server is manipulated or accessed erroneously either by accident or with malice	??
<i>Risk 2:</i> (IBC Note to user: include this row, provided by FullTech May 2020)  Cloud is hacked	??
Risk 3:	
Risk 4:	

## PART 9: SIGNATURES

(IBC note that can be deleted after completing the form: We have been advised by Privacy Officer that IBC does not complete Part 9 – the OCIO would normally complete these parts. However, IBC is not required to have OCIO or any party sign off on our PIAs.)

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

### Privacy Office Comments

### Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
<b>Privacy Officer / Privacy Office Representative</b>			

### Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

### Program Area Comments:

Role	Name	Electronic signature	Date signed
<b>Initiative lead</b>			
<b>Program/Department Manager</b>			
<b>Contact Responsible for Systems Maintenance and/or Security</b> Only required if they have been involved in the PIA			
<b>Head of public body, or designate (if required)</b>			

July 26, 2024

Spencer Izen  
Legal & Social Science Researcher  
Freedom of Information and Privacy Association, Vancouver, BC

**Subject: FIPA FOI 219 Request dated May 28, 2024**

Dear Spencer,

Thank you for the inquiry and granted extension. Below is Innovate BC's reply:

We are responding to your request for information email dated May 28, 2014 regarding *Freedom of Information and Protection of Privacy Act* ("**FOIPPA**") records and descriptions from 1 January 2021 through to 21 May 2024.

As a BC Crown Agency, Innovate BC relies on established policies and procedures by the provincial government as they relate to FOIPPA and the Information Management Act. We do not develop separate policies.

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

We do not have responsive records as requested.

**2. Interoffice memoranda about freedom of information and records/information management.**

Responsive records include:

- a. Staff email regarding FOIPPA training from Innovate BC's Director of Compliance + Governance and Operations Manager (July 2021)
- b. Staff presentation on Protection of Privacy and FOIPPA Overview (2021)
- c. Instructions and link to Privacy and Information Sharing Training (the course is provided by the Province, which Innovate BC staff are required to complete as part of their onboarding)
- d. New Employee Checklist
- e. Privacy Impact Assessment (template and instructions)
- f. Data standardization presentation for staff by Data Analyst (2023)
- g. Decision memo on the transition to MS Teams for internal staff communications
- h. Email to staff regarding the transition from Slack to MS Teams (April 2024)

**3. Metadata Application Profiles and records disposition models, as well associated policies and procedures and implementation plans and reports.**

We do not have responsive records.

Innovate BC relies on government policy for retention and disposition of records, including Record Management Guidelines and Learning, Canada Revenue Agency and other applicable regulations.

**4. Office of primary responsibility designations/matrices.**

We do not have responsive records.

**5. Policies and procedures regarding eDiscovery/Legal Requests for Records.**

We do not have responsive records.

**6. Technical manuals for records management systems.**

Responsive record include:

- Information Security Policy

Yours truly,



Tomica Divic

Vice President, Strategic Partnerships and Ecosystem Development