

[[Initiative Name]] Privacy Impact Assessment

|  |  |
| --- | --- |
| Initiative title: |  |
| Department or Faculty: | [enter four letter code] |
| Administrative Authority | [[The Administrative Authority (as defined in [Policy GV0235](https://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf)) responsible for the initiative.]] |
| Initiative Lead(s) and Contact Information  | [[The person(s) responsible for developing this initiative and for answering questions. Provide name, title, and contact information]] |
| Privacy and Access Office Assessor | Leave Blank |
| PIA Number | To be assigned |

The *Freedom of Information and Protection of Privacy Act* requires that a Privacy Impact Assessment to be conducted for any new Initiative for which no PIA has previously been conducted, or a significant change to an existing Initiative, before implementing the Initiative or significant change.

“Initiative” means a program or activity that involves the collection, use, or disclosure of Personal Information, but does not include the collection, use, or disclosure of Personal Information for research conducted by a faculty member, teaching assistant, or research assistant.

If the Initiative does not involve the management of personal information then only Part 1 must be completed.

If the Initiative involves the storage of sensitive personal information outside of Canada, the General Counsel or their delegate will use the information in the PIA to determine whether to proceed with the initiative based on a risk assessment.

The PIA must be signed by the Administrative Authority responsible for the Initiative, after considering the recommendations of the Corporate Privacy Officer and Chief Information Security Office, as applicable.

Contact privacyinfo@uvic.ca for assistance completing this PIA.

# **PART 1: GENERAL INFORMATION**

## **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.**

[Enter description here]

## **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?**

[Enter scope here.]

1. **What are the data or information elements involved in your initiative?**

**Please list all the elements of information or data (both personal and non-personal information) 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. Determine the Information Classification for each element according to the** [**University Information Security Classification Procedures**](https://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf) **in IM7800.**

|  |
| --- |
| Table 1 – Information elements |
| Line | Information or Data | Further description, if needed | Classification |
| 1 |  |  | Highly Confidential/ Confidential/Internal/ Public |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |

### **Did your information list in question 3 include personal information?**

[**Personal information**](https://www2.gov.bc.ca/gov/content?id=45F56451625849E49141D4AF85D8EEC2) **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 no, answer [question 4](#_How_will_you) and submit the PIA with your answers to questions 1 to 4 and signed by the Administrative Authority to privacyinfo@uvic.ca. You do not need to complete the rest of the PIA template**.**

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

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

[Describe strategies to reduce risk here]

**IF THERE IS NO PERSONAL INFORMATION, STOP HERE**

# **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.

## **Collection, use and disclosure**

List all data flows in the table below. A data flow is either a **collection**, a **use**, or a **disclosure** of personal information by UVic or by a UVic contractor. Add as many rows as necessary to the table to comprehensively describe the flow of personal information in the initiative.

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. In many cases, you may not know the FIPPA authority. If this is the case, leave the column blank for the CPO to complete.

| **Table 2 – Data Flows** |
| --- |
| **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** | **FIPPA authority** | **Other legal authority** |
| 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.

## **Collection**

**Are you collecting all of the personal information used in your initiative directly from the person the information is about? If no, list the sources of the personal information referencing back to the relevant step in the data flow table in question 5.**

[describe sources of indirect collection here]

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

Review the sample collection notice and write your collection notice below. Alternatively you can also attach the notice as an appendix.

The University of Victoria will be collecting your personal information for the purposes of [**INSERT PURPOSE HERE**]. This information is collected under [CPO will **INSERT FIPPA SECTIONS HERE**] of the *Freedom of Information and Protection of Privacy Act*. If you have any questions or concerns about how your personal information is handled please contact privacyinfo@uvic.ca.

# **PART 3: SECURITY OF PERSONAL INFORMATION**

In Part 3 you will provide details about 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 secured according to its Information Security Classification in both physical and technical environments.

## **Does your initiative involve sensitive personal information?**

Sensitive personal information is any personal information classified as “Highly Confidential” under IM7800, or that is about an individual’s health, finances, race, ethnicity, or other characteristic that if disclosed could result in harm to an individual.

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

If yes, list the line(s) in Table 1 that are sensitive.

Line(s):

## **Is personal information stored by a service provider?**

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

* If no, go to [question 10](#_Does_the_contract" \o "question 12)
* If yes, fill in the table below (add more rows if necessary) and go to [question 9](#_Will_the_service)

| **Table 3 – PI Stored by Service Provider** |
| --- |
| **Name of service provider** | **Name of underlying cloud infrastructure and/or platform provider(s) (if applicable)** | **Where is the personal information geographically stored (including backups)?** |
|  |  |  |
|  |  |  |

## **Will the service provider disclose personal information to a third party subcontractor.**

Service providers often use sub-contractors to process personal information in order to provide service to UVic. For example, a service provider may use a sub-contractor for analytics, or for sending emails. If the service providers discloses personal information to subcontractors list the subcontractors below.

| **Table 4 – Third Party Subcontractor Access to Personal Information** |
| --- |
| **Name of subcontractor** | **Purpose pf disclosure to subcontractor** | **Where is the personal information geographically stored by the subcontractor?** |
|  |  |  |
|  |  |  |

## **Does the contract with the service provider include UVic’s** [**Privacy Protection Schedule**](https://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf) **and** [**Cloud Security Schedule**](https://www.uvic.ca/systems/assets/docs/pdfs/informationsecurity/uviccloudsecuritystandard.pdf)**?**

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

* If No, describe the privacy management program and information security controls in place with the service provider. You may need help from the Privacy and Access to Information Office and University Systems.

## **If no service provider is used to store the personal information, or if you are storing some personal information on campus, what technical and physical security do you have in place to protect personal information** **in accordance with the Information Security Classification Procedures?**

 (Skip this question if you are using a service provider/contractor)

Describe where the 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.

### 11.1 Does the system storing this information meet UVic’s Information Security Standards?

## **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.

| **Table 5 – Controlling and Tracking Access** |
| --- |
| **Strategy** |  |
| We only allow employees in certain roles access to information |  |
| * How many employees have access to the information?
 |  |
| Employees that need standing or recurring access to personal information must be approved by the Administrative Authority |  |
| We use audit logs to see who accesses a file and when |  |
| **Describe any additional controls:** |  |

## **If your initiative stores sensitive personal information, provide specific details about how access to the sensitive personal information is controlled and tracked.**

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

If the initiative will store personal information outside of Canada, the General Counsel of Corporate Privacy Officer must first determine whether the storage is authorized, based on an evaluation of the risk associated with storage, the steps taken to mitigate the risk, and the benefits of the initiative. This section will collect information for that determination.

## **Is any sensitive personal information stored outside of Canada?**

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

* If Yes, go to question on to 15.
* If No go to [Part 5](#_Risk_Response_for).

## **Provide specific details about how access to the sensitive personal information is controlled and tracked.**

## **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.

|  |
| --- |
| **Table 6 – Details of Privacy Risks** |
| **Privacy risk**  | **Impact to individuals** | **Likelihood (low, medium, high)**  | **Risk Level (considering impact and likelihood)**  | **Strategies employed to mitigate the risk** **(this may include contractual mitigations, technical controls, and/or procedural and policy barriers)** | **Residual risk after mitigation?** **If yes, please describe.**  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Outcome of Part 4**The outcome of Part 4 will be **a risk-based decision made by the Corporate Privacy Officer on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks.  |

# **PART 5: ACCURACY, CORRECTION AND DISPOSITION**

In Part 5 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete and is not retained for longer than required.

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

**FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual’s personal information is accurate and complete.**

[Explain how you will ensure accuracy]

## **Requests for Correction**

**FIPPA 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.**

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

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

### **Sometimes it’s not possible to correct the personal information. FIPPA 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.]

###  **If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA 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.]

## **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 19](#_What_Directory_of)
* If no, skip ahead to [Part 7](#_PART_7:_SIGNATURES)

## **What Directory of Records classification(s) applies to the information?**

**FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition,** [**IM7700 – Records Management Policy**](https://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf) **requires that you dispose of information only in accordance with the** [**Directory of Records**](http://www.uvic.ca/dor)**. Contact** **rmhelp@uvic.ca** **if you have questions about records management or the Directory of Records.**

List DoR entries that apply, add new rows if necessary.

| **Table 7 – Directory of Records** |
| --- |
| **DOR Classification** | **(Retention and) Disposition requirements** |
|  |  |

1. **If you are using a software platform or storing information with a service provider, does the platform or service provider have the ability to delete information?**

**[Answer Yes or No].**

# **PART 6: ADDITIONAL RISKS**

Part 6 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.

## **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.

| **Table 8 – Risk Response** |
| --- |
| **Possible risk** | **Response** |
| Risk 1: |  |
| Risk 2: |  |
| Risk 3: |  |
| Risk 4:  |  |

# **PART 7: COMMENTS**

*Once completed and reviewed by the Privacy and Access to Information Office, include the recommendations or comments of the CPO and CIO or CISO, and have the PIA signed by the Administrative Authority responsible for the initiative.*

## **Data Protection Officer Comments**

## **Corporate Privacy Officer Comments**

## **Chief Information or Chief Information Security Officer Comments**

## **Department Comments**

# **PART 8: 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 the Privacy and Access to Information Office and if necessary, complete a PIA update.

By signing below the Administrative Authority assumes responsibility for the privacy risk associated with this initiative.

| **Table 10 – Signatures**  |
| --- |
| **Role** | **Name** | **Electronic signature** | **Date signed** |
| **Administrative Authority** |  |  |  |
| **Data Protection Officer** |  |  |  |
| **Corporate Privacy Officer or General Counsel** |  |  |  |