Privacy Impact Assessment Guidelines

for Insurers Looking to Implement Usage-Based Insurance Programs in Alberta

January 2016

Office of the Information and Privacy Commissioner of Alberta

Contents

Introduction

This document was prepared by the Office of the Information and Privacy Commissioner (OIPC) to provide Privacy Impact Assessment (PIA) drafting guidance to insurers who may decide to prepare and submit a PIA to the OIPC ahead of offering usage-based insurance (UBI) in the province of Alberta.

UBI is a type of automobile insurance where insurers consider additional rating factors to determine the level of insurance premiums to be paid by policy holders. UBI programs involve the collection, use and disclosure of information pertaining to the operation of a motor vehicle by individuals.

The *Personal Information Protection Act* (PIPA) protects the personal information of individuals held by private sector organizations in Alberta by establishing rules for how organizations collect, use and disclose personal information about their clients, customers and employees. The Act balances the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.

The next sections of this document will provide you, as the individual(s) preparing a PIA on behalf of an insurer in relation to the introduction of a UBI program, with greater details about the PIA process, as well as details about the expected content and format of the documentation.

PIA Process

The PIA is a due diligence exercise, in which you identify and address potential privacy risks that may occur in the course of your operations, or in the course of the operations of any other agent you contract services to. The PIA process requires a thorough analysis of potential impacts to privacy and a consideration of reasonable measures to mitigate these impacts.

While PIAs are focused on specific programs, the process must also include an examination of organization-wide practices that have an impact on privacy. Your policies and procedures, or the lack of them, affect your ability to ensure that privacy protecting measures are applied to specific programs.

1. *Personal Information Protection Act*

As defined in section 1(1)(i)(i) of PIPA, insurers licensed in Alberta pursuant to the *Insurance Act* of Alberta are “organizations”. As such, insurers must follow the rules in PIPA regarding the collection, use, disclosure, security, retention and destruction of the personal information in their custody or under their control.

PIPA requires organizations to obtain consent for the collection, use, or disclosure of personal information, except in limited circumstances. PIPA also provides individuals with a right to

request access to their personal information, and to learn how that information has been used and to whom it has been disclosed.

If an individual believes an organization has failed to comply with its obligations under PIPA, the individual can ask the OIPC to review the actions of the organization. The OIPC has the powers to investigate, hold inquiries, and issue binding orders.

Under Alberta's PIPA, PIAs are not mandatory. However, the PIA process is a valuable tool to help you assess your program's compliance with PIPA.

The OIPC reviews PIAs under the authority of section 36(1)(f) of PIPA to comment on the implications for protection of personal information in relation to existing or proposed programs of organizations.

2. Making a PIA Submission

Submit your PIA to the OIPC under the signature of the individual designated to ensure your organization's compliance with PIPA. The OIPC may return a PIA that has not been submitted by a person with appropriate authority.

Incomplete PIA submissions will be returned to the submitter without being reviewed. This applies particularly to submissions that are missing policy and procedure attachments listed in Section E of the PIA template.

PIAs submitted in relation to the introduction of UBI programs should follow the format described in this document and be submitted to the OIPC at the following address:

Office of the Information and Privacy Commissioner of Alberta
410 - 9925 109 St NW
Edmonton AB T5K 2J8

3. PIA Review

After receiving a PIA, a Senior Information and Privacy Manager from the OIPC is assigned to conduct a review. The Senior Information and Privacy Manager may raise questions or seek clarification on certain points in your PIA. This may occur if the program's legal authorities are unclear or missing, if impacts to privacy are significant and unmitigated, or if the risks to privacy appear to outweigh the benefits of the program. The Senior Information and Privacy Manager may contact you by phone, fax, email, or letter.

4. OIPC Review Time

Be sure to allow time for the OIPC to review and comment on your PIA so you can consider this feedback before you fully implement your program. If you leave it too late and the OIPC

identifies privacy concerns, it may be necessary to make expensive and time-consuming changes to your program late in the development cycle.

The OIPC will try to provide the preliminary results of your PIA review within 45 calendar days. The duration of the PIA review process depends on the accuracy and completeness of your PIA, and on how quickly you resolve any questions raised by the reviewing Senior Information and Privacy Manager.

5. PIA Comments

Once you address any questions and are committed to providing the necessary level of privacy protection, the reviewing Senior Information and Privacy Manager accepts the PIA by sending you a letter to confirm. Acceptance is not approval; it reflects the Senior Information and Privacy Manager's opinion that you have considered the requirements of PIPA and have made a reasonable effort to protect privacy. A PIA cannot be used to obtain a waiver of, or relaxation from, any requirement of PIPA, or to prevent a review by the Commissioner if an individual files a privacy complaint.

If you do not respond to all questions raised in the PIA review within the deadlines set by the Senior Information and Privacy Manager, your PIA review file will be closed without acceptance. It is difficult to demonstrate that you have taken reasonable measures to protect privacy when your PIA has not been accepted. This situation can put your program at risk, especially if you face privacy complaints from the public.

6. Changes to Your UBI Program

New practices and technologies evolve after programs are implemented. New threats to privacy may also develop over time. You may also change third party service providers.

You should periodically review your PIA to ensure any risks caused by changes such as these are addressed. You should also advise the OIPC of any resulting changes to your PIA. In some cases a short letter is sufficient; in other cases, you may wish to resubmit a revised PIA.

If a member of the public makes a complaint against your organization, the Commissioner or OIPC staff may review previously submitted PIAs to gather information about your privacy practices.

If you have questions about the PIA process or requirements, you may visit the OIPC website at www.oipc.ab.ca or contact the OIPC by phone at 780-422-6860 or by email at generalinfo@oipc.ab.ca.

PIA Submission Overview

The OIPC expects that you follow the format described in this document for any Privacy Impact Assessment (PIA) prepared in relation to the introduction of a usage-based insurance program in the province of Alberta.

PIA submissions must include the following sections. Each section is described in more detail in the rest of this document.

Cover Letter

- The cover letter is a brief letter, addressed to the Information and Privacy Commissioner that introduces the PIA. It is signed by the head of the organization submitting the PIA, or their authorized representative.

Cover Page

- The cover page provides basic information about the PIA and contact information for people involved in the PIA process.

Section A

- 'Program Overview' describes the program to be assessed in plain language.

Section B

- 'Privacy Management' addresses the overall management of privacy functions within the organization, including the related organizational structure and policies.

Section C

- 'Program Privacy Analysis' addresses privacy topics related to the specific program that is the subject of the PIA.

Section D

- 'Program Privacy Risks and Mitigation Plans' describe the privacy risks and mitigation measures you have identified for the program in question. This is a critical component of the PIA and should be completed in as much detail as possible.

Section E

- 'Policy and Procedures Attachments' provides a list of privacy and information security policies you need to attach to your submission. Policies and procedures specific to the program are also included in this section.

Cover Letter

Organize your PIA using the titles and headings in this section, in the same order that they appear here.

Submit your PIA with a cover letter signed by someone with executive authority to do so. In most cases, this is the head of the organization or someone who has been formally authorized to act on the organization's behalf; for example, legal counsel, or the Chief Privacy Officer.

The person with primary responsibility for the PIA may be the same person primarily responsible for privacy legislation compliance.

Cover Page

Please include the following information on your cover page:

- official program name, including any other names or acronyms commonly used to refer to the program;
- legal name of the organization that prepared the PIA;
- name, title and full contact information of the person with primary responsibility for completing the PIA (it will normally be whoever wrote the PIA or performs the role of privacy officer or privacy coordinator, and will be the OIPC's primary point of contact for any questions about the PIA);
- name, title and full contact information of the person with primary responsibility for privacy legislation compliance; this could be the Chief Privacy Officer, or his or her authorized representative;
- PIA submission date; and
- expected program implementation date (for information technology programs, this is the date when your production system goes into use with live data).

Section A: Program Overview

Describe the proposed program, including its objectives. State why the program must collect, use or disclose personal information.

Your overview should answer some basic questions about the program that triggered the PIA.

- How does the program work?
- What is the business rationale for the program?
- Who is involved in program delivery, both inside and outside the organization?
- Where will personal information be stored/accessed?

- Why does the program need to collect, use or disclose particular personal information data elements to achieve its objectives?

- Why does the program need to collect, use or disclose the amount of personal information to achieve its objectives?

The OIPC publishes summaries of all accepted PIAs in an online PIA Registry. The information you provide in this section may be posted in the PIA Registry on the OIPC's website.

Section B: Organizational Privacy Management

You do not need to list your privacy and security policies here; you will have an opportunity to do that in Section E of your PIA.

If you have already provided a description of your privacy management in a previous PIA and no changes are needed, you may reference the previous PIA using the OIPC file number.

1. Management Structure

How is your senior management involved in decision-making related to privacy?

Describe your senior management team's engagement in setting privacy policy and resolving privacy issues.

For example, who does your privacy officer or privacy coordinator report to? Is there a privacy committee? You may include an organization chart showing how the privacy function is positioned in your management structure.

2. Policy Management

How do you develop, approve and implement privacy policies?

Describe how policies are developed, who approves them, how they are communicated, how often they are reviewed, and any other relevant information concerning the privacy policy environment.

3. Training and Awareness

How are your employees and contractors trained in privacy?

Identify privacy training you give your employees and contractors, such as new employee orientations and on-going privacy awareness programs.

You should note who receives training, how often you offer training, whether your training program is periodically updated to reflect legislative and technology changes, and how you document that someone has received privacy training.

4. Incident Response

How do you identify, investigate and manage privacy incidents?

The OIPC defines a privacy incident as an event that adversely affects the confidentiality, integrity or availability of personal information. A privacy incident may result in the collection, use, disclosure, or loss of personal information in contravention of PIPA.

Describe your approach to privacy incident response. Your description should state what triggers your incident response plan, who is involved in incident response, how you decide to notify affected parties, and how you learn from incidents to improve your privacy practices.

Note: Under section 34.1 of PIPA, it is mandatory to report to the Office of the Information and Privacy Commissioner, without unreasonable delay, any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there is a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. The approach your organization takes when responding to incidents must address this requirement.

More information on mandatory privacy breach notification under PIPA can be found on the OIPC website at www.oipc.ab.ca.

5. Access and Correction Requests

How do you manage requests from individuals to access their own personal information and to make corrections?

Under PIPA, individuals have a right to access their own personal information subject to limited and specific exceptions, and a right to ask for corrections. These rights help to protect individuals' privacy by giving them the ability to see exactly what personal information an organization holds about them, how that information has been used, and to whom it has been disclosed. This helps individuals make decisions about how much information to share and may alert them to potential privacy concerns.

Describe who in your organization is responsible for responding to access and correction requests, how you inform people about your decisions to grant or refuse access/corrections and whether you have an informal process for routine requests.

Section C: Program Privacy Analysis

1. Personal Information Listing

List the personal information that is collected, used or disclosed as part of your UBI program.

Provide a list of all information you are collecting, using or disclosing that falls within the definition of "personal information" in section 1(1)(k) of PIPA.

As you compile your list, make sure you have a defensible reason to collect, use or disclose each piece of personal information in your program. Under PIPA, an organization may collect, use, and disclose personal information only for purposes that are reasonable, and only to the extent that is reasonable for meeting the purposes for which the information is being collected, used or disclosed. When reviewing your PIA, the OIPC may ask you how the listed personal information contributes to the objectives of your program.

For some programs, complete listings of every data element are too lengthy to be useful. In such cases, you may summarize by providing a description of personal information types with some examples in each category.

In all cases, you must list unique identifiers. Unique identifiers are data elements that uniquely identify a single individual. For example, this could include a unique number assigned to a customer, a vehicle identification number, a policy account number, an international mobile subscriber identity (IMSI) number, etc.

Note: In 2011 ABCA 94, the Court of Appeal of Alberta has said *in obiter* that a vehicle identification number (VIN) would not constitute personal information.

2. Information Flow Analysis

Provide a description of the flow of personal information for your UBI program. Support your description with a diagram and table that describe the purposes and legal authority for each collection, use and disclosure of personal information.

To complete this part of the PIA, you need to include two components: an information flow diagram and a table showing the purposes and legal authority for each information flow.

a. Component #1: Information Flow Diagram

An information flow diagram illustrates how personal information is collected, how it is used, and how it is disclosed beyond your program or organization.

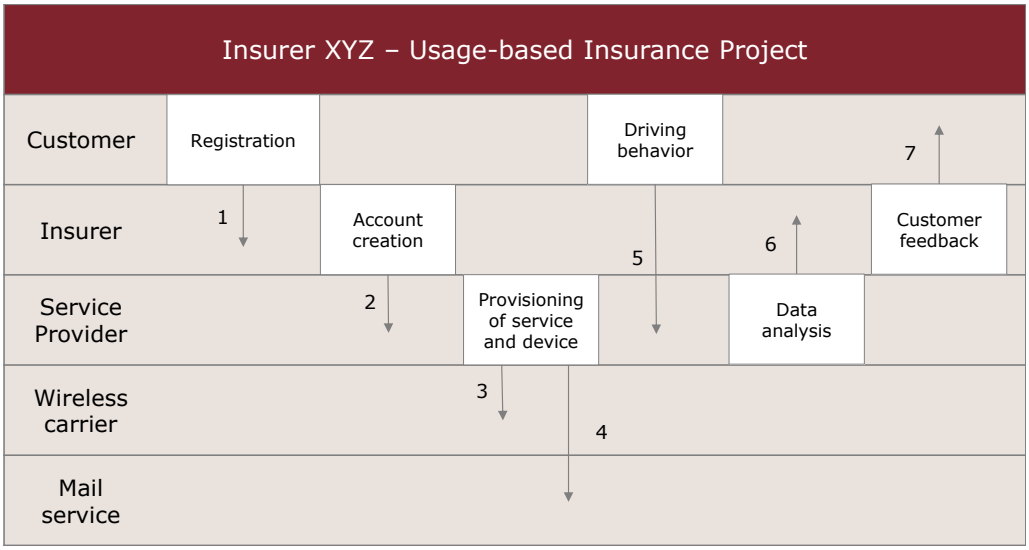
There is no universally accepted format for information flow diagrams, but work flow diagrams, technical data flow diagrams (such as those prepared during the design of

computer applications) or network diagrams, are not likely appropriate for PIA purposes.

The example given below shows one approach to personal information flow diagrams; you may use another method if it makes sense for your program.

This UBI program will:

- collect personal information from customers;
- use this information to provide each customer with a device to plug in their vehicle, which includes disclosing some personal information to service providers;
- collect information about how each customer's vehicle is driven;
- send personal information to a service provider for analysis;
- after service provider has completed analysis of data, it is sent to the insurer; and
- give each customer feedback on their driving behavior, and potential insurance discounts.



Be sure to number each information flow (each collection, use and disclosure) for easy reference.

You will need to refer to each flow in a table that describes its purpose and legal authority.

b. Component #2: Legal Authority and Purposes Table

PIPA sets out general purposes for the collection, use and disclosure of personal information.

Collection, use or disclosure of personal information must be authorized under PIPA. Under PIPA, an organization must have the individual's consent in order to collect, use or disclose personal information, or meet the requirements of section 14, 17 and 20 respectively to collect, use or disclose personal information without consent.

The table below documents that each category of personal information is collected, used or disclosed for a clearly defined purpose. Each purpose must be supported by your legal authority to collect, use or disclose personal information.

Example table: legal authority and purpose table

For each flow of personal information in the diagram above, this table provides details about the purpose of collection, use or disclosure and the corresponding legal authority.

Info Flow #	Description	Type of Information	Purpose	Legal Authority
1	*Customer registers for program*	*Name, DOB, DL #, address, phone #, driving history, claims history, bank account #*	*personal information collected to sign up customer*	*Consent or authority under section 14 of PIPA to collect without consent*
2	*Registration validated and account created/modified*	*Name, address*	*Validate registration and get customer the telematics device they need*	*…*
3	*Service provider fulfils order by provisioning account and configuring device*	*…*	*…*	*…*
4	*Shipping*	*…*	*…*	*…*
5	*Device use*	*…*	*…*	*…*
6	*Service provider processes customer data and provides it to insurer*	*…*	*…*	*…*
7	*Insurer uses data to provide feedback and offer discounts to customer*	*…*	*…*	*…*

3. Notification Required for Collection

Before or at the time you collect personal information from an individual, you must notify that individual as to the purpose(s) for which you are collecting his or her personal

information, as well as give the individual the name or position or title of someone who is able to answer on behalf of the organization the individual's questions about the collection.

Describe how you will notify individuals of all purposes for which their personal information is collected.

Identify measures you take to ensure individuals are informed about how you will use their personal information (written notices, scripted oral notification, posters, web pages, etc.).

Consider any unique needs of individuals or groups in relation to this program. Depending on the scope of the program or unique privacy risks, a general notice may be appropriate in some situations, while other programs may need a specific privacy statement.

Your notice needs to include:

- a description of the purposes for which personal information is collected; and
- contact information for someone who can answer questions about the collection of personal information.

4. Consent

Except where PIPA says otherwise, organizations must get consent to:

- collect personal information;
- collect personal information from someone who is not the individual;
- use personal information; or
- disclose personal information.

Describe how you administer consent in your program.

Consent may be given in writing, orally, or by electronic means. However you collect consent, you need to consider how you will keep a record and how individuals can withdraw their consent. Please refer to the OIPC website at www.oipc.ab.ca for guidance on consent.

5. Contracts and Agreements

Describe contracts or agreements with third-parties involved in your program. Describe the privacy provisions that bind third parties to your own requirements for privacy protection.

You are responsible for ensuring that any of your service providers comply with PIPA in relation to the services they provide on your behalf. Your agreements with third parties, such as service providers for IT support or other services, should include provisions binding providers to a standard of privacy protection equivalent to your own.

Attach copies of your third-party agreements to your PIA submission. At a minimum, you should provide the provisions from these agreements that are related to information handling and privacy.

6. Use of Personal Information Outside Canada

Your organization may need to engage a service provider outside Canada who will have access to personal information in your custody or control. Collecting, transferring or storing personal information outside Canada is permitted under PIPA, but requires careful consideration to assess and mitigate risk. This is particularly important as the laws that protect privacy in other countries may not be equivalent to those in Alberta or Canada. Therefore, your organization's policies and practices must include information about the countries outside Canada in which service providers operate, and information about the purposes for which these service providers are retained.

Out-of-country disclosures may occur in ways you have not considered. For example, if your computer helpdesk is outside Canada, personal information may flow outside the country during helpdesk calls. Also, your data backup or archiving facility may be located outside of Canada.

If your organization directly or indirectly relies on a service provider outside Canada to collect, use or disclose personal information about an individual that was collected with the individual's consent, under section 13.1 you must notify the individual in writing or orally of:

- the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada; and
- the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.

Be sure you have considered all possible collections, disclosures or uses of personal information taking place outside Canada and provide an appropriate notification to individuals where required, in addition to the requirements in the section above.

Section D: Program Privacy Risk Mitigation

1. Access Controls

Describe how persons, positions, employee categories or third parties are given access to specific personal information data elements or categories. This describes your application of the "need-to-know" principle. Personal information should only be accessible to those who have a business need and who have been properly authorized. It is important that you describe who has access to the information, the nature of the information, the circumstances under which they have access, the type of access and the purpose or reason for the access.

Provide a description of the processes used to authenticate user identity and authorize user access to system screens, reports and features. You should also describe how user authorization is terminated when someone leaves or changes position. Include clear descriptions of the access controls themselves and how they are implemented and maintained for the program.

Use an access table based on the following example to answer this question. The table below is for illustration only; you may need to adjust it to provide room for your responses.

Example Table: Access to Personal Information by Role

The table summarizing access controls does not have to reflect the exact number of individuals with each permission level. The intent is to describe the ways in which access to personal information is controlled within the organization.

Position	User Role	Number of staff in this role	Type of Access (Read, Write, Edit)	Description of Information this User Can Access (include examples)
Sales representatives	*Register new customer with the program*	*50*	*Read, write*	*Customer demographics, contact information*
Customer Support				
Data Analytics Specialists				
Customer Service Support				
Service Provider IT Support				
Service Provider System Administrator				

2. Privacy Risk Assessment and Mitigation Plans

Every organization that collects, uses or discloses personal information is inherently exposed to some privacy risks. PIPA does not require that you completely eliminate all risk. Rather, your organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Describe the specific privacy risks you have identified for this program and how you plan to mitigate them. Your response to this question should describe the measures you are taking to address specific privacy risks associated with your UBI program.

a. Program Privacy Risks

Based on the experience of the OIPC, most programs face the five risks listed below. Your mitigation plans must address each of these risks.

1. unauthorized use of personal information by internal or authorized parties;
2. unauthorized collection/use/disclosure of personal information by external parties;
3. loss of integrity of personal information;
4. loss, destruction, or loss of use of personal information; and
5. your service provider or business partner collects, uses or discloses personal information in contravention of applicable privacy legislation or your policies.

If any of these risks do not apply to your program, please explain why.

The above risks are broad. You should describe the circumstances that lead to the risks within your program. For example, you may face the risk of unauthorized use of personal information by external parties because of your reliance on the public Internet, or because the personal information may be a valuable target to hackers because it may be used for fraud.

Your mitigation plans must include a combination of administrative, technical or physical measures you have taken to mitigate or reduce privacy risks.

You will likely have more than one measure to address each risk. For example, you may have a policy combined with a training program and an audit to reduce a particular risk.

Please provide a specific reference to a page number and heading or section number if you refer to attached policies and procedures as part of your mitigation plans.

b. Other Privacy Risks

You will likely identify risks beyond the five listed above. For example, re-identification of anonymized data, theft or loss of mobile devices, or unauthorized disclosure via a wireless network may be risks that are unique to your program.

This is a sample risk mitigation table:

Privacy Risk	Description	Mitigation Measures for Program	Policy Reference
Unauthorized use of personal information by internal or authorized parties	*Staff member uses personal information available to them for reason unrelated to work*	*Employee confidentiality agreement signed* *Audit logging allows detection of unauthorized access*	*Policy ABC* *Policy DEF*
Unauthorized collection/use/disclosure of, or access to, personal information by external parties			
Loss of integrity of personal information			
Loss, destruction, or loss of use of personal information			
Your contractor or business partner collects, uses or discloses personal information in contravention of applicable privacy legislation or your policies			
Other privacy risks specific to your program			

3. Monitoring

Describe your plans to monitor compliance with your privacy protection measures. Include a description of the monitoring processes you will use, how frequently you will apply them, and how you will review results to improve the privacy and security of personal information.

Monitoring is essential to test and improve your ongoing privacy compliance. Provide a program-specific monitoring/audit plan, describing who will conduct reviews, the frequency of monitoring, what kind of anomalies will be flagged for review, and when your incident response plan will be triggered.

Your plans to monitor access, collection, use and disclosure should reflect the sensitivity of the personal information involved. Sensitive information, such as financial information, demands more rigorous monitoring than less sensitive information, such as contact information (however, some circumstances may even require strict monitoring of contact information). Your plans may include internal system log reviews and audits, or independent third party audits.

4. PIA Compliance

Describe how you will periodically review your PIA and communicate updates or revisions to the OIPC as necessary. Also describe how you will monitor your compliance with the statements made in the PIA and make any necessary changes.

Your PIA describes your program, usually just before implementation. Over time, business processes and practices will change and your implemented program may no longer be accurately reflected in your PIA. Similarly, risks and the measures available to mitigate those risks will also change, as a result of new knowledge, new technologies, or other changes to the environment.

It is important to plan for periodic reviews of your program post-implementation to ensure it still conforms to your PIA. If there are gaps between what you described in your PIA and current reality, consider writing a PIA amendment. It is mandatory under PIPA to protect personal information that your organization is responsible for by making reasonable security arrangements; periodic reviews of privacy protection measures, which include your PIA, will help you meet this requirement.

The following examples of changes to an insurer's UBI program would be situations where a PIA amendment would be warranted:

- changing service provider;
- collecting, using, or disclosing more personal information; or
- collecting, using, or disclosing personal information in a different way.

Section E: Policy and Procedures Attachments

Attach copies of policy documents to demonstrate you have addressed the topics listed in the appendices. Use the following table to summarize all of the policy and procedure documents you provide with your PIA.

1. Privacy Policy Table

For each topic in the table, indicate whether you have an applicable policy or procedure and, if so, the title of the document and relevant page reference(s). Your policies and procedures

may respond to more than one of the topics in the table below. If so, please cross reference those policies or procedures to avoid duplication in your responses. However, make sure that you provide page numbers for any cross references to allow easy identification of the relevant material.

2. General Privacy Policies

The table starts with general privacy policies. These are your organizational privacy policies that should be in place without regard to any specific PIA you may prepare.

3. Program Specific Policies

The second part of the table allows you to enter program-specific policies. These are privacy and information security policies that only apply to the program covered in this PIA.

4. Previous PIA Submissions

If there are no changes, you may refer to general privacy policies submitted in a previously accepted PIA.

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Privacy accountability	This is a broad policy that enables privacy roles and accountability within your organization. Sometimes called a privacy charter, this policy does not provide detailed work instructions, but rather sets out responsibilities and commitments in relation to privacy. This policy should include: ▪ where privacy fits into your organizational structure; ▪ who is responsible for privacy, including who is responsible for responding to privacy complaints; ▪ who is responsible for information security; ▪ commitment to protect confidentiality and to collect, use and disclose personal information in a limited manner; ▪ commitment to maintain accuracy of personal information; ▪ commitment to provide privacy training and awareness to employees; ▪ commitment to maintain technical and administrative safeguards to protect personal information; ▪ right of access to personal information and right to request corrections; and ▪ schedule for periodic review of privacy policies.		
Access to personal information	Your process and timeframes for responding to formal requests from individuals for access to their own personal information. Include references to policies for charging fees to process access requests. If you require that individuals fill out a form to make access requests, include it here. You should also consider a process for responding to informal requests or making routine disclosures to individuals.		
Correction requests	Your process and timeframes for responding to individuals who ask you to correct their personal information. Include your process for responding to these requests and describe how you inform individuals of your decisions to grant or refuse corrections.		

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Training, awareness and sanctions	Your privacy training program for employees and others that will have access to personal information in your custody. This policy should include sanctions for not complying with your privacy policies.		
Collection of personal information, notification and consent	Acceptable reasons for collecting personal information, which should include consent or statutory authority, under PIPA or other relevant legislation. Include examples or descriptions of how you obtain the consent of individuals when you are collecting their personal information, and how you notify individuals of the purposes for the collection. Describe how you notify individuals about non-Canadian service providers, if applicable.		
Use of personal information	Acceptable uses of personal information in your organization.		
Disclosure of personal information	Reasons why your organization discloses personal information to other organizations or persons. This policy should cover: ▪ disclosure with consent; ▪ disclosure without consent; and ▪ disclosure of non-identifying information.		

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Service providers	How you ensure that contractors and service providers protect your organization's personal information. This policy should include: ▪ privacy requirements for service providers; and ▪ review of service provider compliance.		
PIAs	Circumstances that trigger your organization to conduct a Privacy Impact Assessment. This policy should describe who is responsible for conducting PIAs and how often they are reviewed.		
Records retention and disposition	How long you keep records containing personal information and what you do with them once they are no longer needed. Include references to any statutory or professional records retention and disposition schedules you follow. This policy should also include a process to securely dispose of personal information when no longer needed.		
Information classification	Information should be protected at a level commensurate with its sensitivity and the risks it faces. Describe how you classify personal information in order to determine the most appropriate level of security.		
Risk assessment	New risks to the confidentiality, integrity and availability of personal information may arise over time as technology and business processes evolve. This is your policy for conducting periodic risk assessments to assess the effectiveness of your privacy policies.		

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Physical security of data and equipment	The physical and administrative measures you take to secure personal information in paper and electronic form. This policy should describe how you secure your workspaces, computers, fax machines, copiers, and other office equipment. Pay special attention to securing mobile equipment, such as smartphones, tablets, notebook computers and mobile data storage devices.		
Network and communications security	Measures you take to secure your network and communications infrastructure. This could include such controls as malware (anti-virus) protection, firewalls, intrusion detection systems and encryption.		
Access controls	Identifying and verifying users of your personal information, deciding what information they need to use, and making changes when users change positions or leave. Identification and verification includes assigning usernames, passwords and tokens.		
Monitoring and audit	How you ensure that users of personal information comply with your policies. This policy should describe what you monitor to ensure compliance, frequency of review and triggers for a formal audit/review or activation of your incident response plan.		

Topic	Policy Description	Attachment Title(s)	Page Reference(s)
Incident response and notification	Your plan to deal with contraventions of applicable privacy legislation or your own privacy policies. Your plan should: ▪ define what constitutes a privacy incident (or levels of privacy incidents); ▪ identify members of an incident response team; ▪ describe process to bring incidents to attention of senior management and engage them in response; and ▪ include the process to notify Office of the Information and Privacy Commissioner and individuals about the incident, where there is a real risk of significant harm to the individuals.		
Business continuity	How you ensure personal information is available when needed. This includes your plans to back-up data and your plans for disaster recovery, based on business need.		
Change control	Ensuring that changes to systems do not adversely affect the confidentiality, integrity or availability of personal information.		
Other program-specific policies	Include program-specific policies here.		