# Privacy Management Program Framework

## The City of Calgary

# contents

# Introduction

The City of Calgary's ("The City's") *Privacy Management Program Framework* reflects The City's commitment to achieve compliance with the *Freedom of Information and Protection of Privacy Act* ("FOIP Act") of Alberta, earn and maintain trust by exceeding privacy requirements prescribed by legislation and be transparent about The City's internal governance structures and privacy practices.

This *Privacy Management Program Framework* is intended to supplement The City's *Privacy Charter*, by providing more in-depth information about The City's internal key practices related to collection, use, disclosure and retention of personal information designed to achieve the following five (5) purposes set out in the FOIP Act:

A right of access to records

Protection of personal privacy

A right of access to an individual's own personal information

A right to request a correction

Independent review of decision

The *Privacy Management Program Framework* is divided into three (3) parts:

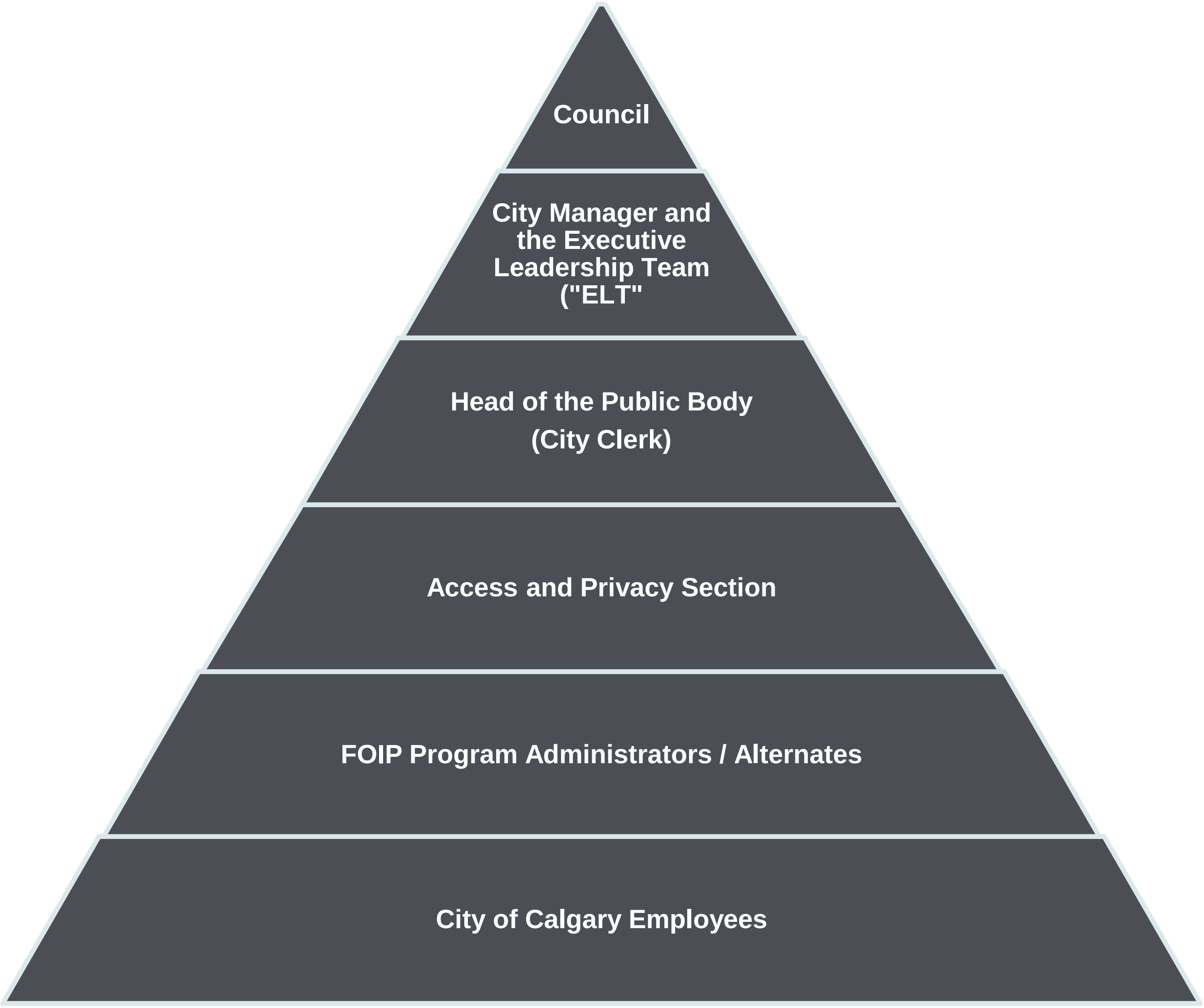
i. The City of Calgary Privacy Commitment;
ii. Privacy Controls and Practices; and
iii. Privacy Monitoring and Improvement.

Each part of the *Privacy Management Program Framework* describes core privacy practices and processes, and provides operational privacy tools, such as templates, guides, forms, tip sheets and links to additional resources, in an effort to be transparent about how The City handles personal information and to assist City employees in establishing and maintaining good privacy practises across the organization.

# Part I: The City of Calgary Privacy Commitment

# i. Organizational Structure

The City has a governance structure in place to ensure compliance with the FOIP Act, and to promote The City's Privacy Vision, Privacy Principles and the *Privacy Management Program Framework*:


Council
City Manager and the Executive Leadership Team ("ELT"
Head of the Public Body
(City Clerk)
Access and Privacy Section
FOIP Program Administrators / Alternates
City of Calgary Employees

# ii. Key Partnerships

To effectively manage privacy and enable The City's Privacy Vision and Privacy Principles, including Privacy by Design[1], key partnerships within The City are essential. The City's *Privacy Management Program Framework* relies on collaboration with the following key partners:

- Corporate Analytics and Innovation
- Corporate Security
- Environmental and Safety Management
- FOIP Program Administrators ("PA") and Alternates
- Human Resources
- Information Management Services and City of Calgary Archives
- Information Technology
- Law
- Supply

[1] Privacy by Design Centre of Excellence. Ryerson University. Available online

# Part II: Privacy Controls and Practices

# i. Legislation and Policies

## Legislation

**Alberta's *Freedom of Information and Protection of Privacy Act* ("FOIP Act")**
The FOIP Act sets out the following five (5) purposes:

1. **A right of access to records** in the custody or under the control of a public body subject to limited and specific exceptions as set out in the FOIP Act;

2. **Protection of personal privacy** by controlling the manner in which a public body may collect, use, and disclose personal information;

3. **A right of access to an individual's own personal information,** subject to limited and specific exceptions as set out in the FOIP Act;

4. **A right to request a correction** to an individual's personal information that is held by the public body; and

5. **Independent review of decisions** made by a public body under the FOIP Act and for the investigation of complaints. Independent review is provided by the Office of the Information and Privacy Commissioner ("OIPC") of Alberta.

The FOIP Act further provides that the head of the public body must protect personal information by making reasonable security arrangements against any risks, including unauthorized access, collection, use, disclosure, or destruction of personal information.

## Policies

The City has a number of privacy-related policies, developed collaboratively across the organization, focused on ensuring compliance with the FOIP Act and alignment with industry best practices:

- ***Privacy Impact Assessment Policy***
- ***Acceptable Use of City Technology Resources Policy***
- ***Information Management and Security Policy***
- ***Protecting Cardholder Data Policy***
- ***Records Management Policies:***
    - *Records Disposition*
    - *Records Management Program Mandate and Responsibilities*
    - *Vital Records Management*
    - *Archival Records Management*
    - *Electronic Records Management*
    - *Transitory Records Management*

City Administration policies are approved by the ELT, and are available to City employees and the public.

# ii. Directory of Personal Information Banks

The City's new digital *Directory of Personal Information Banks* will bring The City into compliance with the FOIP Act and promote transparency about the kinds of personal information collected, reasons for collection and how the personal information will be used by The City.

The *Directory of Personal Information Banks* includes, for each Personal Information Bank, the following:

- the title and location of the personal information bank
- a description of the kind of personal information and the categories of individuals whose personal information is included
- the authority for collecting the personal information
- the purposes for which the personal information was collected or compiled and the purposes for which it is used or disclosed

## Operational Privacy Tool Kit

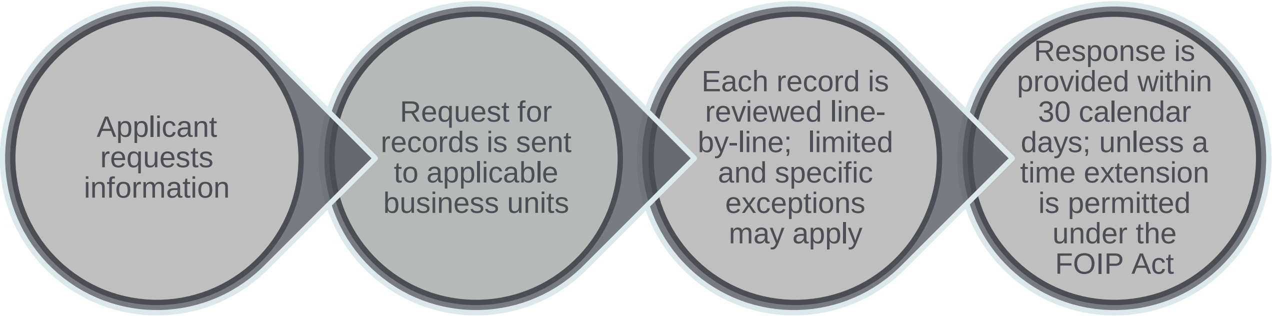
- Personal Information Bank Guide
- Personal Information Bank Template

## Digital Tools for Personal Information Banks

- A digital library that tracks and publishes a Directory of Personal Information Banks across the organization, effective January 2021, to provide City employees and the public with information about The City's personal information holdings and uses, and to assist individuals with exercising their access and correction rights under the FOIP Act.

# iii. Accuracy and Access to and Correction of Personal Information

The FOIP Act provides individuals with a right of access to records in the custody or under the control of The City, subject to limited and specific exceptions set out in the legislation; and with a right to request corrections to their personal information about them held by The City. When The City receives an access to information request, it follows a consistent process for providing access to information:



Applicant requests information

Request for records is sent to applicable business units

Each record is reviewed line-by-line; limited and specific exceptions may apply

Response is provided within 30 calendar days; unless a time extension is permitted under the FOIP Act

Access to information requests provide individuals with access to two different types of records in the custody or under the control of The City:

**General information** is recorded information not about an identifiable individual.

**Personal information** is recorded information about an identifiable individual.

Members of the public and City employees who wish to access and/or correct their personal information can complete The City's Request to Access or Correct Information Form.

## Operational Privacy Tool Kit

- Request to Access or Correct Information form (CC739)
- *Access to Information and Privacy Employee Handbook*
- Service Alberta's *FOIP Guidelines and Practices*
- Service Alberta's *FOIP Bulletins*
- *Privacy Charter*

# iv. Collection of Personal Information

Section 33 of the FOIP Act provides that no personal information may be collected by or for a public body unless:

- the collection of that information is expressly authorized by an enactment of Alberta or Canada;
- that information is collected for the purpose of law enforcement; or
- that information relates directly to and is necessary for an operating program or activity of the public body.

Personal information must be collected only in accordance with the provisions of the FOIP Act. The City's *Privacy Charter* provides information on why The City collects personal information, when it collects personal information, as well as a list of examples. The FOIP Act sets the rules on how The City collects personal information:

**Minimum Collection**

The City only collects the minimum amount of personal information required for the operating program or activity of The City.

**Direct Collection**

The City only collects personal information directly (some exceptions may apply under the FOIP Act).

### Direct Collection of Personal Information – Notice

When collecting personal information, a notice of collection is provided informing individuals of:

a. the purpose for which the information is collected;
b. the specific legal authority for the collection; and
c. the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Notice is given prior to collection, and may be given in manners appropriate to the situation and context. Generally, notice is provided on City forms, brochures, handouts, on posters in public areas, and anywhere information is collected electronically. In certain circumstances, it may be provided verbally.

The City is committed to consistency across all City departments and programs in order to help City employees and the public receive similar notices no matter where collection occurs within The City.

### Operational Privacy Tool Kit

- *Access to Information and Privacy Employee Handbook*
- Access to Information and Privacy Awareness online training
- Service Alberta's *FOIP Guidelines and Practices*
- Model Agreement and Release authorization form

# v. Retention and Disposition of Personal Information

The FOIP Act provides that if an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must retain the personal information for at least one year after using it to make a decision, so that the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by:
a. the individual,
b. the public body,
c. if the body that approves the records and retention and disposition schedule for the public body is different from the public body, that body.

## Retention

Managing records disposition is part of The City Records and Information Management Program. The City's mandate is to retain City records until they have met operational, legal, fiscal and archival requirements as set out in the Corporate Records Classification and Retention Schedule ("CRCRS").

The classification and retention policies for The City are set out in City of Calgary Bylaw 53M99, being a bylaw to adopt policies and procedures for the management of The City's records, including classification and retention schedule, and in seven (7) accompanying Administration policies. Guidance for City employees is an important part of ensuring that retention schedules are adhered to in order to retain personal information only for the amount of time that is required for operational, legal, fiscal and/or archival purposes.

## Disposition

Corporate records are retained until they have met operational, legal and fiscal value to The City, at which time they are disposed of by destruction, deletion or transfer to The City's Archives. The disposition process ensures that corporate records are retained and disposed of in accordance with the CRCRS and ensures the appropriate handling of confidential materials and the transfer of records designated for permanent preservation to Archives. Disposition of records may be delayed or suspended as a result of an audit, a legal action, a change in legislation, an access to or correction of Information request, or a change in the use of a record or record series.

When records have met their retention requirements, the disposition process is implemented. Disposition of records requires the appropriate approvals and sign-off at The City, as outlined in The City's *Records Disposition* policy (GN-013(B)). This Administration policy also ensures that any destruction carried out in accordance with the CRCRS is appropriate for the type of record, and that appropriate security measures are observed for the disposition of records containing personal or other confidential information.

## Decommissioning Databases

Database records can be fully decommissioned once the official records in the database have met retention requirements or, in the case where some of the database official records have not met retention requirements, the remaining records are moved to another repository. A disposition form will be used to authorize decommissioning/disposition of information a Business Unit is responsible for, once retention requirements have been met.

# vi. Protection of Personal Information

The FOIP Act requires that the head of a public body must protect personal information by making reasonable security arrangements against such risks as:

- unauthorized access;
- collection;
- use;
- disclosure; or
- destruction

## Physical

Access and authorization mechanisms (for example, employee access cards) are in place to limit access to only authorized individuals. Physical Security Risk assessments are completed on priority sites and physical security systems are in place to protect sites and information assets. Secure filing rooms and cabinets are provided for personal information storage which include access control mechanisms.

## Technological

The City's information assests are controlled and protected. With the extensive use of third-party technologies, services and tools, we provide:

- access controls on devices
- access control for applications and databases
- risk management
- intrusion protection
- usage restrictions
- virus protection
- network security
- multi-factor authentication

## Administrative

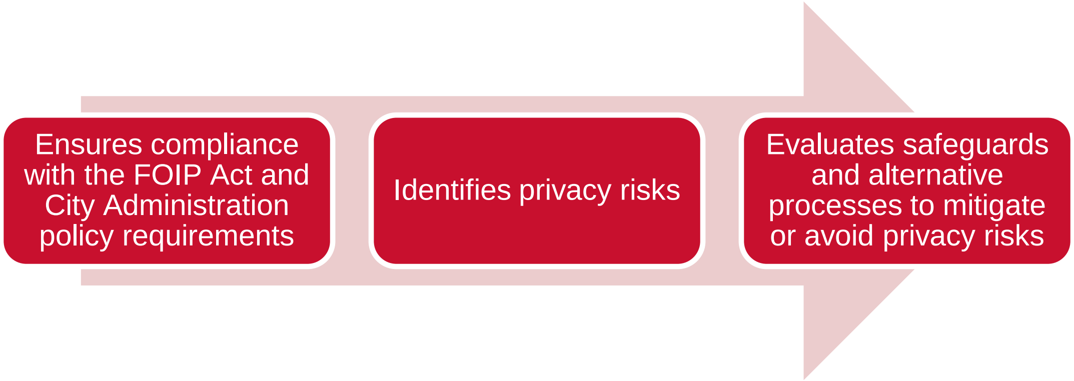
City employees and third parties contracted by The City have access to Administration policies, including Privacy Impact Assessments, and training to bring awareness to their responsibilities related to information management, security and privacy. Our Administration policies identify roles and responsibilities, as well as provide direction to staff on how to protect personal information. Resources are in place to support information sharing with suppliers, vendors and contractors, including contractual obligations stipulating confidentiality and security of information, as well as privacy breach protocol.

# vii. Privacy Impact Assessments

Essential to The City’s commitment to protecting personal information of citizens and employees, and making reasonable security arrangements against unauthorized access, collection, use, disclosure or destruction, is identification and mitigation of privacy risks in any new or updated project, process, initiative and information technology.

The City’s primary tool for identifying privacy risks is a Privacy Impact Assessment (“PIA”). While a PIA is not a requirement under the FOIP Act, The City adopted an Administration policy on *Privacy Impact Assessments* requiring all City projects, practices and information technology systems that involve the collection, use or disclosure of personal information to undergo a PIA.

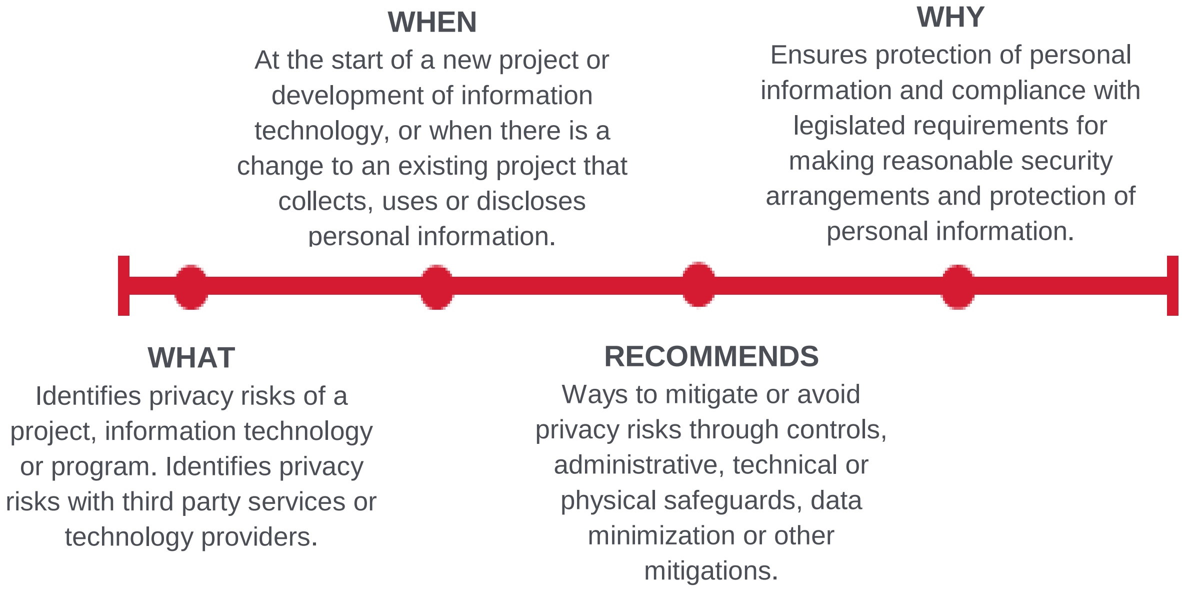
A PIA helps facilitate Privacy by Design and builds privacy directly into The City’s practices and technologies at the outset and not as an afterthought. A PIA:



Ensures compliance with the FOIP Act and City Administration policy requirements

Identifies privacy risks

Evaluates safeguards and alternative processes to mitigate or avoid privacy risks



**WHEN**

At the start of a new project or development of information technology, or when there is a change to an existing project that collects, uses or discloses personal information.

**WHY**

Ensures protection of personal information and compliance with legislated requirements for making reasonable security arrangements and protection of personal information.

**WHAT**

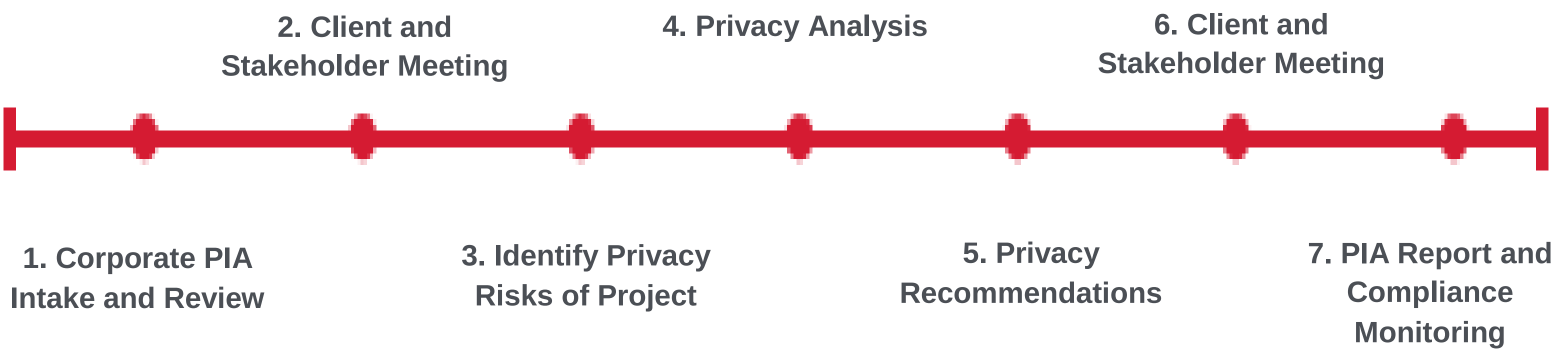
Identifies privacy risks of a project, information technology or program. Identifies privacy risks with third party services or technology providers.

**RECOMMENDS**

Ways to mitigate or avoid privacy risks through controls, administrative, technical or physical safeguards, data minimization or other mitigations.

# Privacy Impact Assessments

## The PIA Process



1. Corporate PIA Intake and Review

2. Client and Stakeholder Meeting

3. Identify Privacy Risks of Project

4. Privacy Analysis

5. Privacy Recommendations

6. Client and Stakeholder Meeting

7. PIA Report and Compliance Monitoring

## Operational Privacy Tool Kit

- PIA Intake Form (CC929)
- PIA Report
- PIA Summary Document
- Privacy Tip Sheet: Privacy Impact Assessments
- Access to Information and Privacy Awareness Training
- *Access to Information and Privacy Employee Handbook*
- OIPC's *"Privacy Impact Assessment Requirements" Guide*
- Service Alberta's *FOIP Guidelines and Practices*

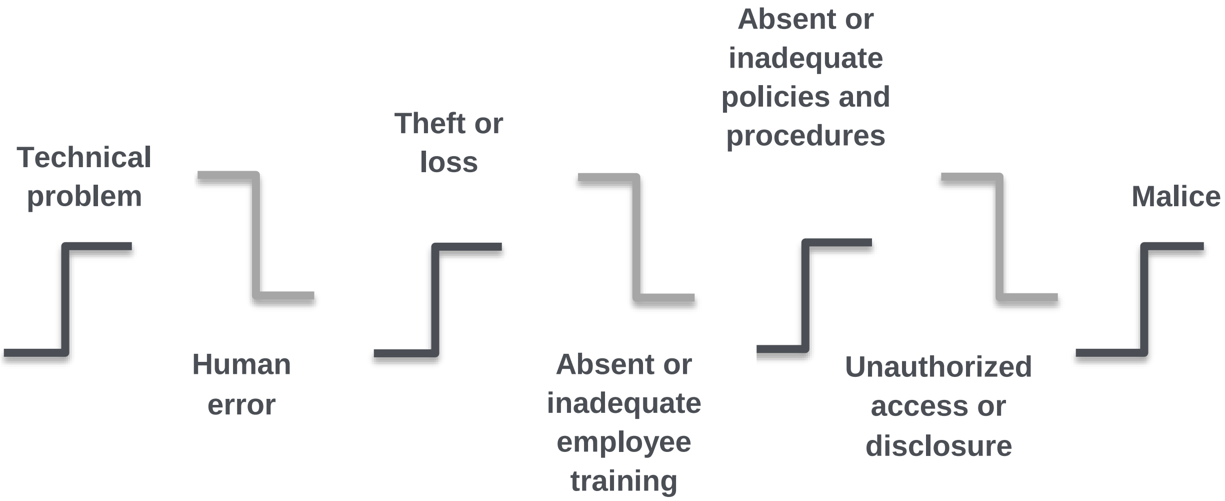
## Digital Tool for PIAs

- A digital library that tracks and manages accepted PIAs for City projects, programs, services and technologies involving personal information collection, use and disclosure. The digital library contains accepted PIAs since January 1, 2018
- A complete list of accepted PIAs, since January 1, 2018, and PIA Summaries, since January 1, 2021, are now available on calgary.ca, providing the public with information about how The City handles their personal information in City projects, programs, services and technologies

# viii. Privacy Complaint Management

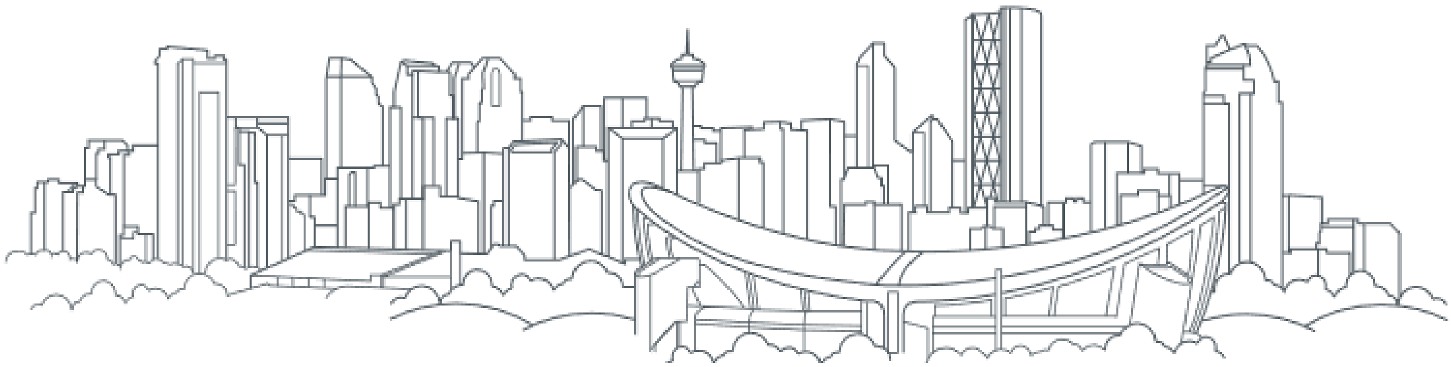
The City is committed to safeguarding personal information and making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction.

There may be times when The City's reasonable security safeguards (administrative, technical and/or physical) may be compromised, inadequate, missing or subject to malice, and a privacy breach occurs. A privacy breach means a loss, unauthorized access to or disclosure of personal information. The City's definition of privacy breach is aligned with that of the OIPC of Alberta. Generally, privacy breaches can occur as a result of:


Technical problem
Human error
Theft or loss
Absent or inadequate employee training
Absent or inadequate policies and procedures
Unauthorized access or disclosure
Malice

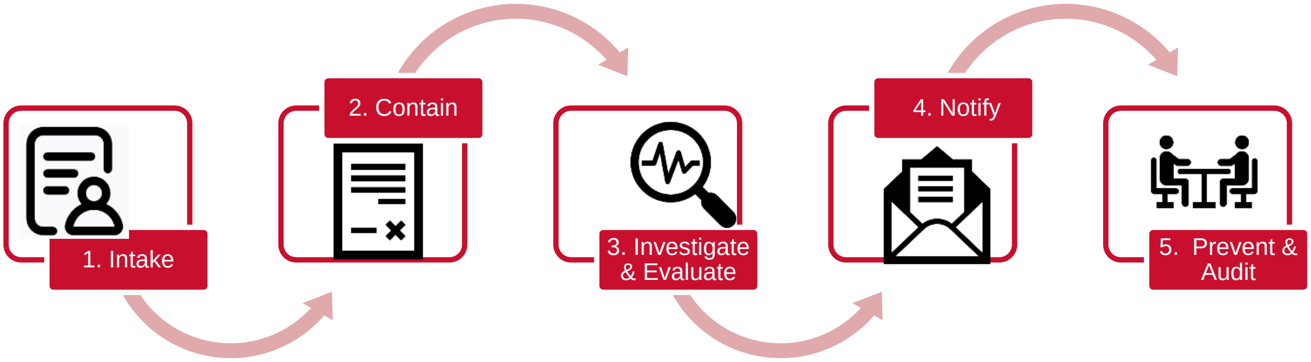
The City has mechanisms in place to:

- Enable citizens and City employees to raise privacy concerns regarding compliance with the FOIP Act or The City's privacy practices;
- Bring awareness to City employees' requirement to report all privacy concerns, including suspected privacy breaches; and
- Take urgent action to contain, investigate, notify and prevent future privacy breaches.



# Privacy Complaint Management

## Privacy Breach Response Process



### 1. Intake

The City has an established intake process to receive confidential privacy complaints from members of the public and City employees. The City has mechanisms in place, a *Privacy Complaint Report Form for Members of the Public* and a *Privacy Breach Report Form for City Employees*, to assist with documenting a privacy complaint. The City's forms collect the following information, and supporting evidence may be required, to aid with an investigation into a privacy complaint:

- Incident description;
- Personal information involved;
- Safeguards;
- Harm;
- Risk assessment;
- Containment; and
- Notification, if necessary.

Members of the public and City employees also have the right to notify the Alberta OIPC. If a privacy complaint is investigated by the OIPC, The City fully cooperates with the Information and Privacy Commissioner's investigation.

# Privacy Complaint Management

## 2. Contain

Once a privacy breach has been identified, it is important to take immediate actions to contain the privacy breach, if possible, and notify a Supervisor and the Access and Privacy Section. This step ensures that any potential or real harm to the affected individual(s) or others is minimized. The Access and Privacy Section will assist business units in containing the privacy breach and will coordinate with key partners, when required. If the privacy breach is a result of theft or other criminal activity, business units should notify the Calgary Police Service.

## 3. Investigate and Evaluate

The investigation process determines what other actions are needed. An evaluation of risks associated with a privacy breach is always completed, including but not limited to the following:

Personal information elements involved?

Scope and number of affected individuals?

Cause and extent of the privacy breach?

Possible harm?

## 4. Notify

The FOIP Act does not impose mandatory requirements on The City to notify either the affected individual(s) or the Alberta OIPC. Although not required by law, notification to individual(s) may be an important risk mitigation strategy. The City notifies affected individual(s) and/or the OIPC following a comprehensive assessment of a real risk of significant harm to an individual as a result of personal information loss, unauthorized access or disclosure.

# Privacy Complaint Management

## Notification to an Affected Individual

Content of The City's notification to affected individual(s) will vary depending on the nature of the privacy breach and the method of notification. Generally, notification will include the following elements set out by the Alberta OIPC[2]:

- Date of the privacy breach
- Description and general circumstances of the privacy breach
- Description of the personal information involved in the privacy breach
- The steps The City has taken to contain the privacy breach and minimize any potential harm
- The steps the affected individual can take to further mitigate the risk of harm
- Next steps planned by The City, including any long term plans to prevent privacy breaches
- Contact information for The City's FOIP Coordinator who can answer questions
- That individuals have a right to contact the OIPC, including the OIPC's contact information

Generally, notification is provided by The City's FOIP Coordinator/Deputy City Clerk directly to the affected individual in writing; however, there may be circumstances where indirect notification is given via Calgary.ca, posted notices or the media.

[2] Key Steps to Responding to Privacy Breaches. OIPC. August 2018. Available online.

# Privacy Complaint Management

## Notification to the Information and Privacy Commissioner

Content of The City's notification to the OIPC will vary depending on the nature of the privacy breach. Generally, the following factors set out by the Alberta OIPC are considered in making the determination with respect to notification[3]:

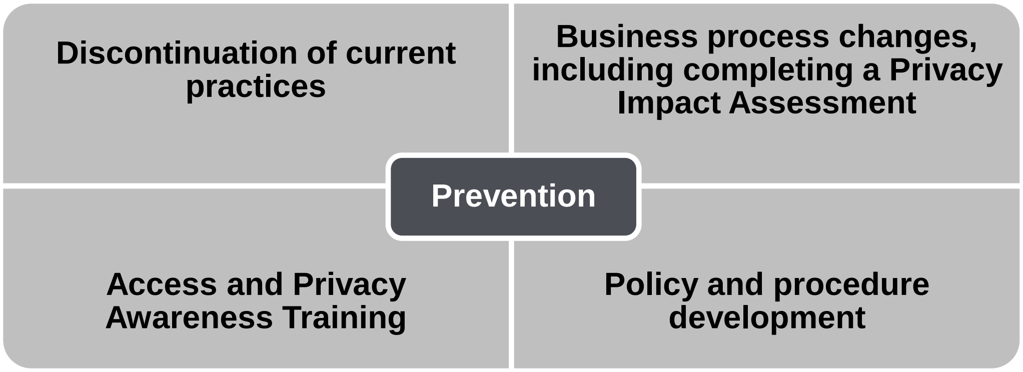
- Type of personal information involved in the privacy breach
- Whether the disclosed personal information could be used to commit identity theft, fraud, embarrassment, hurt or humiliation, mental or physical harm, or financial harm
- Whether the disclosed personal information could be used to damage reputation or relationships
- Whether there is a reasonable chance of harm from the privacy breach
- The number of people affected by the privacy breach
- Whether vulnerable individuals, such as seniors or youth, were affected by the privacy breach
- How long the personal information was exposed and to whom
- Whether there is evidence of malicious intent or purpose, such as theft, hacking or malware
- Whether the personal information was recovered without futher disclosure

[3] Key Steps to Responding to Privacy Breaches. OIPC. August 2018. Available online.

# Privacy Complaint Management

## 5. Prevent and Audit

Following containment, investigation and evaluation, time is taken to thoroughly analyze the privacy breach and develop recommendations with respect to what measures and/or safeguards could be taken to prevent future privacy breaches. Recommendations can include but are not limited to:



Prevention

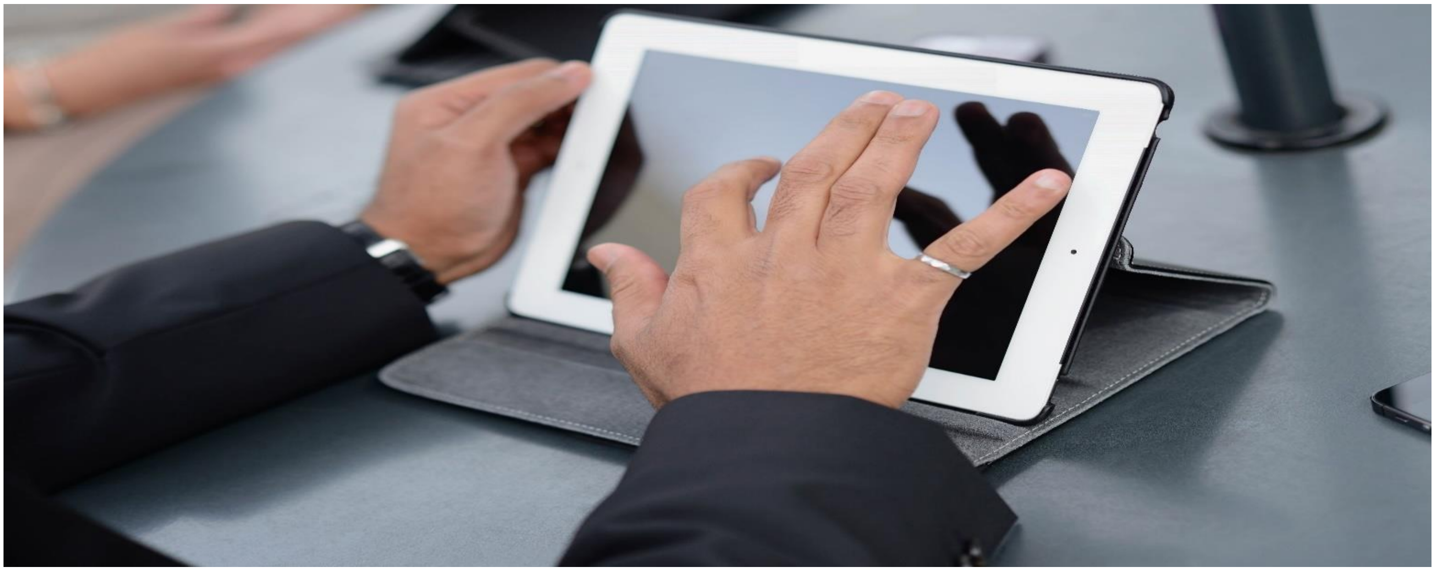
Discontinuation of current practices

Business process changes, including completing a Privacy Impact Assessment

Access and Privacy Awareness Training

Policy and procedure development

The resulting Letter of Findings, containing the recommendations to mitigate against future privacy breaches, includes an auditing requirement to ensure that the preventative strategies or safeguards have been fully implemented.



# Privacy Complaint Management

The roles and responsibilities with respect to managing the privacy breach response at The City are defined as follows:

### Access & Privacy Team

- Review privacy complaint reports;
- Implement containment measures to limit privacy breach;
- Investigate and evaluate privacy breaches;
- Offer privacy breach mitigation; recommendations to business units;
- Conduct compliance audit reviews.

### FOIP Program Administrators (PA)/Alternates (Alt)

Assist their respective business unit in reporting, containing and preventing a privacy breach, including suspected privacy breaches

### FOIP Coordinator/Deputy City Clerk, Information and Privacy

- Makes decisions and issues notification to affected individual(s) and/or the OIPC; and,
- Establishes a Privacy Breach Response Team as required.

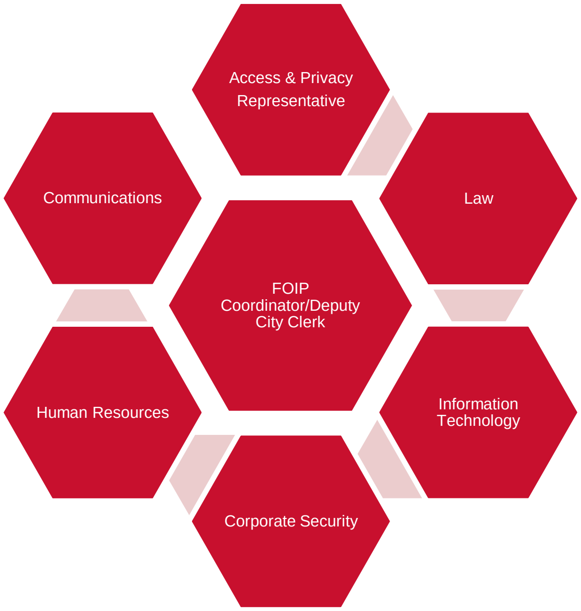
### Head of the public body/City Clerk

- Maintains overall accountability for privacy breach response; and
- Escalates privacy breach matters to Senior Leadership and Council.

## Privacy Breach Response Team

Depending on the circumstances of the privacy breach, a privacy breach response team may be established to carry out containment, notification and to minimize any current, ongoing or future risks associated with a privacy breach.

Membership of a privacy breach response team varies depending on the context, and may include the following:



### Operational Privacy Tool Kit

- •Privacy Complaint Report Forms: Members of the Public (CC950) and City Employees (CC822)
- •Privacy complaint form (OIPC)
- •10 Privacy Tips: *Sending emails and best practices to protect personal information*
- •Privacy Awareness online training

# ix. Use of Third-Party Services or Technologies

### Third Party Protection of Personal Information

The City may engage third-party service providers to supply a service which is managed by The City. In these instances, the third-party service provider is an ‘employee’ of The City, and as such, has a duty under the FOIP Act to protect the personal information that it collects, uses and discloses as part of that service. Privacy awareness training is available to third party providers.

By engaging in the PIA process when selecting service providers, The City can ensure service providers limit the collection of personal information, have adequate safeguards in place to protect the personal information it collects, uses, and discloses on behalf of The City, and will dispose of the personal information after the business purpose for the collection has been completed.

Information Technology’s Cloud Computing and Open Source Program helps Business Units evaluate third-party providers.

### Data Protection of Personal Information

Information security design is part of all systems and infrastructure architecture design; Information Technology technical processes, business practices and methodologies follow City policies and standards; and plans for business continuity are in place. All data located on City websites and in email, software applications, databases, files (documents, spreadsheets, images, etc.) and other information repositories supported by Information Technology are managed, protected and monitored. Third-party technologies provide, but are not limited to:

Email protection from spam and malware

Secure processing of financial transactions

Reporting and alerts

Various means of restricting changes to our systems

Secure web traffic transmission and protection of files

### User Authentication

Systems and procedures are in place to authenticate users. The City requires user name and a unique password, two-factor authentication (for remote access), certificate, external token, or biometrics before access is granted to systems handling personal information.

# Use of Third-Party Services or Technologies

### Device Management

Information Technology uses tools to manage The City's desktop, laptop and thin-client computers which provide standardization for how they are built and installed, hard drive encryption, enforcement of security rules, regularly updated security patches, and the ability to lock them down remotely in the event of theft and remote administration and monitoring.

To help ensure business continuity and protection of data, Information Technology keeps The City's third-party technologies and services up-to-date and stable to ensure the latest security protections are in place. This includes operating systems, servers, databases, computers and mobile devices, as well as The City's wired and wireless networks.

City Administrative policies restrict the use of unapproved hardware and software for storing personal information. This includes personal devices, removable media (thumb drives) and hosted software without appropriate identity management and authentication.

### Logging and Monitoring

User access to personal information (e.g. viewing, modification, deletion of records) both from a front-end (e.g. business user) perspective and a back-end (e.g. system or database administrator) perspective is logged and monitored on a regular basis in accordance with the Access Control Standard (Information Management and Security Policy). Efforts are underway to ensure all locations and systems which contain personal information generate logs which are directed to a security and event monitoring process to identify unauthorized access or suspicious user activity. These events are monitored and reviewed by the Corporate Security Information Security Operations Team.

### Change Control

Information Technology maintains a change control process which ensures that new implementation and modifications to systems follow strict change control processes to ensure system data is not exposed.

# x. Awareness, Education and Training

**The City believes that everyone in our organization has a role to play in protecting personal information. City employees receive training on privacy and reporting privacy complaints. The City is committed to ensuring our employees have access to training and development to protect personal information when developing programs, information technologies or processes, and when handling personal information of citizens and colleagues.**

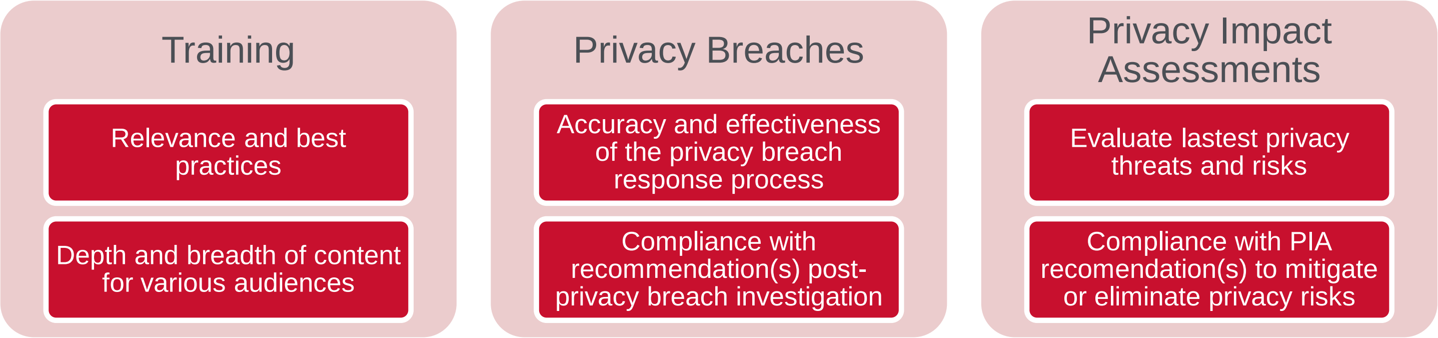
As part of The City's commitment to fostering a culture that respects privacy, we deliver training such as the following to raise privacy awareness amongst employees:

- **City of Calgary Onboarding ("COCO") Welcome Workshop**
- **Code of Conduct Training**
- **Privacy Awareness Training**
- **Access to Information Training**
- **FOIP Program Administrator Training**
- **Information Management & Security Training**
- **Information Management & Security eLearning**
- **Business Unit Specific Access and Privacy Training**
- **Introduction to Records and Information Management and Retention**
- **Introduction to Records and Information Management eLearning**
- **Access to Information and Privacy Handbook for City of Calgary Employees**

# Part III: Privacy Monitoring and Improvement

# i. Monitoring

Monitoring and reviewing the privacy practices set out in this *Privacy Management Program Framework* is important to ensure they remain relevant, effective and contribute to ongoing compliance and accountability. The City is currently monitoring the following privacy practices:



Training

- Relevance and best practices
- Depth and breadth of content for various audiences

Privacy Breaches

- Accuracy and effectiveness of the privacy breach response process
- Compliance with recommendation(s) post-privacy breach investigation

Privacy Impact Assessments

- Evaluate lastest privacy threats and risks
- Compliance with PIA recomendation(s) to mitigate or eliminate privacy risks

| Privacy Program Control[4] | Current Status of Privacy Program Control | Current Monitoring Frequency |
|---|---|---|
| **Policies** | Individual policies in place; Comprehensive Privacy Policy under development | Periodic |
| **Directory of Personal Information Banks** | Implementing in Q1 2021 | |
| **Risk Assessment Tools: Privacy Impact Assessment** | In place | Annual |
| **Training and educational requirements** | In place | Annual |
| **Privacy Complaint Management** | In place | Annual |
| **Service Provider Management, including use of third party services or technologies** | In place | As needed |
| **External communication** | Additional communication tools under development | As needed |

## City Auditor

Bylaw 30M2004 provides the City Auditor and staff with unrestricted access to all municipal personnel, records, property, policies, procedures, processes and systems necessary to conduct audits. The right of access has been granted by Council and cannot be overridden by City Administration. The City Auditor has the authority to audit any area of City operations reporting to the City Manager, including the Privacy Management Program.

[4] *"Getting Accountability Right with a Privacy Management Program".* April 2012. Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia. Available online.

# ii. Improving Privacy Practices

The City is committed to creating a culture of continuous improvement, and encourages input from City employees, the public and privacy experts on The City's *Privacy Management Program Framework*. In 2020, The City conducted research with the public and City employees on key privacy practices, privacy vision, and privacy principles. The outcomes of this research, along with the recommendations of the privacy expert, will be used to develop, enhance and improve the current privacy practices and tools in the years ahead.

The *Privacy Management Program Framework* will be reviewed on an annual basis commencing in 2022. Each year, an oversight and a review plan will be created to monitor, assess and evaluate the following:

- privacy program controls, and update as required
- new opportunities for continous improvement
- evolving information technologies, and new risks or threats to privacy
- provincial, national and international best practices related to privacy