Title:	**Protection of Privacy**
Effective Date:	**2026 June 01**
Responsible Business Unit:	**Law, Legislative Services & Security – Information & Privacy Services**

1. PURPOSE

1.1 The purpose of this Administration policy is to:

a) Set out the roles, responsibilities, and general principles that The City of Calgary ("The City") must follow to ensure compliance with the *Access to Information Act ("ATIA"),* SA 2024, Chapter A-1.4, the *Protection of Privacy Act ("POPA"),* SA 2024, Chapter P-28.5, and the *Protection of Privacy (Ministerial) Regulation ("Ministerial Regulation"),* AR 143/2025;

b) Foster public trust and confidence in The City through openness and transparency regarding the collection and management of personal information, data derived from personal information and non-personal data;

c) Ensure The City takes reasonable security safeguard measures to protect and manage personal information, data derived from personal information, and non-personal data in its custody or under its control against such risks of unauthorized access, collection, use, disclosure, or destruction;

d) Ensure The City is accountable for making reasonable efforts to provide access to personal information, data derived from personal information, non-personal data and records;

e) Communicate expectations for employee conduct as one of The City's Code of Conduct policies; and

f) Set out a Privacy Incident Response Protocol.

2. APPLICABILITY

2.1 This Administration policy applies to:

a) All employees; and

b) All records containing personal information or through which individuals can reasonably be identifiable through the mosaic effect, data derived from personal information and non-personal data, regardless of format or location, that are in the custody or under the control of The City.

2.2 This Administration Policy does not apply to:

a) Elected officials;

b) Calgary Housing Corporation employees; and

c) Calgary Police Service employees.

2.3 If any provision of this Administration Policy conflicts with any provision of *ATIA* and/or *POPA*, the provision of *ATIA* and/or *POPA* prevails.

3. POLICY STATEMENT

Personal Information

3.1 Collection of Personal Information and Notice

a) The City only collects personal information as authorized by law, for the purposes of law enforcement or as is necessary for The City's operating programs or activities.

b) Personal information is collected directly from the individual the information is about, subject to exceptions under *POPA*.

c) When information is collected directly from an individual, notice is given to inform them of the purpose of the collection, the legal authority for the collection, and the contact information of an individual who can answer questions about the collection, subject to exceptions under *POPA*.

d) When information is collected directly from an individual, notice is given, at the time of collection, of The City's intention, if any, at that time to input the information into an automated system to generate content or make decisions, recommendations or predictions.

e) The City is committed to providing a website that respects our visitors' privacy. Collection and management of personal information through the website is based on the legal authority and purpose expressed in the notice in accordance with *POPA*, and the Privacy Policy of the website.

3.2 Use and Disclosure of Personal Information

a) The City will maintain a directory of personal information banks ("PIBs") and make it available to the public.

b) The City may only use personal information to the extent permitted under *POPA*, or other applicable legislation.

c) The City may only disclose personal information as permitted under *ATIA* and *POPA*, or other applicable legislation.

3.3 Sale of Personal Information

a) The selling of personal information in any circumstance or for any purpose, including for marketing or advertising purposes is prohibited.

3.4 Accuracy and Correction of Personal Information

a) The City will make reasonable efforts to ensure that personal information used to make a decision directly affecting an individual is complete and accurate.

b) Individuals shall have the right of access to records in the custody or under the control of The City containing their personal information, subject to limited and specific exceptions set out in *ATIA*.

c) Individuals may request a correction to their personal information if they believe there is an error or omission. A correction request will be handled in accordance with the Correction of Personal Information Standard.

3.5 Retention and Disposition of Personal Information

a) Where The City uses an individual's personal information to make a decision that directly affects the individual, The City will retain the personal information for at least one year after using it.

b) The City will retain and dispose of records containing personal information in accordance with The City's *Retention and Disposition Bylaw* and *Corporate Records Management Administration Policy*.

Data Matching and Data Derived from Personal Information

3.6 Collection or Creation of Data Derived from Personal Information

a) The City may carry out data matching to create data derived from personal information only for research and analysis or planning, administering, delivering, managing, monitoring or evaluating a program or service, or as otherwise permitted under applicable law.

b) When carrying out data matching to create data derived from personal information, The City will only collect personal information from another public body or use personal information in its custody or under its control.

3.7 Use and Disclosure of Data Derived from Personal Information

a) Data derived from personal information may only be used for the purpose for which it was created and as long as is reasonably necessary to enable The City to carry out that purpose.

b) The City will not disclose data derived from personal information, except to another public body from which personal information was collected for the purpose of carrying out data matching to create data derived from personal information and if that public body requires the data for the purpose for which it was created.

3.8 Retention and Disposition of Data Derived from Personal Information

a) As soon as reasonably possible, The City will destroy data derived from personal information or transform it into non-personal information after The City has finished using it for the purpose for which it was created.

Non-Personal Data

3.9 Creation of Non-Personal Data

a) The City may create non-personal data only for research and analysis or planning, administering, delivering, managing, monitoring or evaluating a program or service, or as otherwise permitted under applicable law.

b) When creating non-personal data, obligations respecting the use of generally accepted best practices, quality assurance, and maintaining a creation record will be managed with the Privacy Officer.

c) To create non-personal data, The City will only use personal information or data derived from personal information already in The City's custody or control.

3.10 Use and Disclosure of Non-Personal Data

a) The City may use non-personal personal data it has created for any purpose.

b) The City may disclose non-personal data to another public body for any purpose.

c) The City may disclose non-personal data to a person other than a public body only for the purpose of research and analysis, or planning, administering, delivering, managing, monitoring, or evaluating a program or service.

d) Any disclosure of non-personal data to a person other than a public body must be done in association with the Privacy Officer and only after the person has signed an agreement complying with the approved conditions.

e) The City is not restricted from disclosing reports, summaries or other publications containing non-personal data that is in aggregate or statistical form.

3.11 Protection of Personal Information, Data Derived from Personal Information and Non-Personal Data

a) The City is committed to meeting its legal obligations to have reasonable security arrangements against such risks including unauthorized access, collection, use, disclosure, or destruction of personal information, data derived from personal information, and non-personal data.

b) The City protects personal information, data derived from personal information and non-personal data by implementing physical, technological, and/or administrative safeguards appropriate to the sensitivity of the information.

c) When an applicant makes an access to information request for their personal information, The City will require them to provide acceptable proof to verify the applicant's identity, to show that they are the individual whose personal information is being requested.

d) All contracts entered into by The City that may involve the collection, use, or disclosure of personal information in the performance of the contract, will include a requirement for reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Artificial Intelligence and Automated Systems

3.12 The City will only use personal information in artificial intelligence systems or automated systems in accordance with *POPA*.

Privacy Management Program

3.13 Privacy Management Program ("PMP")

a) The City will establish and implement a PMP consisting of documented policies and procedures that promote The City's compliance with its duties under *POPA*.

b) The City shall make the PMP publicly accessible.

c) The PMP shall be reviewed, assessed and updated from time to time, but no less than every two years.

Privacy Compliance and Risk Assessment

3.14 Privacy Compliance and Risk Assessment Engagement

a) The City will participate in Privacy Compliance and Risk Assessment engagement when a new, or a substantial change to an existing, administrative practice, program, project or service involves the collection, use or disclosure of personal information.

b) Should The City practice, program, project or service meet *POPA* and *Ministerial Regulation* requirements for the preparation of a privacy impact assessment ("PIA") it shall provide a level of detail commensurate with the complexity of the practice, program, project or service.

c) A PIA must be submitted to the Office of the Information and Privacy Commissioner ("OIPC") if one or more factors apply, as prescribed in *POPA* and the *Ministerial Regulation*.

Privacy Incidents

3.15 Privacy Incident Response

a) The City will investigate all privacy-related incidents and may respond to any privacy-related complaint.

b) An investigation is triggered by the submission of a *Privacy Incident Report Form*, through the direction of the OIPC, or the Privacy Officer.

c) Investigation activities may include reviewing and assessing information provided, conducting interviews and gathering evidence to document the events related to a privacy incident.

d) The City's "Privacy Incident Response Protocol" (Appendix 1) describes the roles and responsibilities for managing privacy incidents.

4. ROLES AND RESPONSIBILITIES

4.1 Employees are responsible for:

a) Participating in mandatory privacy awareness training to understand appropriate collection, use, protection, management, disclosure, correction, and disposition of personal information, data derived from personal information and non-personal data;

b) Only collecting, using, and disclosing personal information as authorized by *POPA*, or other applicable legislation;

c) Implementing reasonable safeguards to protect personal information, data derived from personal information and non-personal data;

d) Participating in privacy compliance and risk assessment engagement to help identify and address potential privacy risks with respect to a new, or a substantial change to an existing administrative practice, program, project or service that will involve the collection, use, or disclosure of personal information;

e) Ensuring that the Privacy Officer is engaged in any projects involving data matching or non-personal data;

f) Responding to access to information requests in a timely manner by searching for, documenting, and producing all responsive records;

g) Reporting any privacy incidents to the Privacy Officer, and limiting the scope and impact of any privacy incident when possible;

h) Reviewing privacy recommendations and implementing the recommended privacy risk mitigation strategies where possible; and

i) Making factual corrections to personal information without a formal request under *POPA*, if this is practical and expedites public business, when directly requested by the individual whom the personal information relates to in accordance with the Correction of Personal Information Standard.

4.2 Access and Privacy Program Administrators (“APPA”s) and Alternates are responsible for:

a) Attending APPA specific training, and in consultation with the Privacy Officer, providing corresponding advice and guidance to their business unit regarding compliance with *ATIA* and *POPA*;

b) Seeking guidance from the Privacy Officer regarding new or complex situations involving personal information, data derived from personal information and non-personal data;

c) Leading the business unit response, which includes coordinating the search for, identifying and retrieving records, responsive to access to information requests;

d) Ensuring that information that can be routinely disclosed is identified;

e) Ensuring that the business unit perspective is documented in any recommendation on a response to an access to information request by completing the *Business Unit Records Request ("BURR") Form*;

f) Participating in the Privacy Compliance and Risk Assessment engagement and facilitating the completion and maintenance of business unit inventory of privacy engagement outcomes;

g) Creating or modifying PIBs on behalf of the business unit;

h) Supporting their business unit to protect personal information, data derived from personal information and non-personal data, reporting any suspected or actual privacy incidents, helping with audits and privacy incident investigations, and assisting with implementation of corrective actions;

i) Being the first point of contact with the Privacy Officer for any projects involving data matching or non-personal data; and

j) Conducting regular reviews to ensure compliance with the *Protection of Privacy Administration Policy*, including reporting noncompliance concerns to their director or Privacy Officer when issues arise.

4.3 Business Unit Directors are responsible for:

a) Ensuring the business unit has an APPA and Alternate appointed for their business unit to carry out the duties specified in 4.2;

b) Ensuring all employees receive access and privacy awareness training as applicable for their role; and

c) Ensuring all employees are compliant with the *Protection of Privacy Administration Policy*.

4.4 Head of the Local Public Body ("the Head") is responsible for:

a) Protecting personal information by ensuring reasonable security arrangements are made against such risks as unauthorized access, collection, use, disclosure or destruction of personal information, data derived from personal information, and non-personal data as set out in *POPA*;

b) All obligations of the Head under *ATIA* and *POPA* that relate to The City; and

c) Maintaining an up-to-date delegation instrument for the Head's delegated powers and duties.

4.5 Privacy Officer is responsible for:

a) Developing and implementing policies, guidelines, and procedures to manage The City's compliance with *POPA*;

b) The overall development, implementation, and maintenance of The City's PMP, and ensuring the tasks and responsibilities set out in the PMP are incorporated in The City's organizational structure;

c) Assisting with establishing and endorsing standards and procedures to ensure compliance with the privacy protection measures in *POPA* regarding the collection, use, disclosure, accuracy, retention, and safeguards of personal information, data derived from personal information, and non-personal data;

d) Ensuring The City has policies and procedures for proactive monitoring of information systems that hold personal information, data derived from personal information, or non-personal data;

e) Policies related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data, if The City is using personal information in artificial intelligence systems, the creation of non-personal data or data matching activities;

f) Communicating with the OIPC, including coordinating any negotiations, mediations, inquiries, and investigations on behalf of The City;

g) Leading The City's training on *POPA*, policies, procedures, and tools; and

h) Leading The City's privacy incident response and Privacy Incident Response Team, when required.

5. CONSEQUENCES OF NON-COMPLIANCE

5.1 Employees who fail to adhere to this Administration policy may be subject to corrective action, including dismissal from employment, in accordance with the Labour Relations standard, the Exempt Staff policy, or the specified terms outlined in their employment contract.

5.2 Failure to comply with the duties imposed by *ATIA* and/or *POPA* or otherwise acting in contravention of the legislation may lead to penalties or offences under *ATIA* and/or *POPA*.

6. DEFINITIONS

6.1 In this Administration policy:

a) **Access and Privacy Program Administrator or APPA and Alternate** means the business unit representative(s) appointed to coordinate business unit activities supporting compliance and advancement of the PMP;

b) **Access to Information Request** means a request under ATIA for access to records for general or personal information in the custody or under the control of The City;

c) **Automated System** means any system, software, or process that uses computation as a whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities;

d) **Bargaining Unit** means a group of employees who have a common interest and are represented by a single labour union, with an agreement with The City in collective bargaining and other dealings with management;

e) **Conflict of Interest** means when a person or entity has a private or personal interest that could influence or compete with, or be perceived to influence or compete with, the objective exercise of the privacy incident investigation;

f) **Control** means The City has the authority over the creation, use, distribution, retention, or disposition of the records;

g) **Custody** means records that are in The City's possession and may include records supplied by a third party;

h) **Data Derived from Personal Information** means data created by data matching, and that identifies any individual whose personal information was used in the data matching;

i) **Data Matching** means linking personal information between two or more databases or other electronic sources of information;

j) **Disposition** means the formal process of removing records from business unit custody when the retention period is met, by deletion or destruction, transfer to archival holdings, or transfer to another organization;

k) **Employee** means City staff and any person who performs a service for The City as an appointee, volunteer, or student, or under a contract or agency relationship with The City as per *POPA*;

l) **Head** means the person or group of persons designated by bylaw or other legal instrument to perform the duties of the Head under *ATIA* and *POPA*;

m) **Mosaic Effect** means a concept that illustrates how elements of information may be non-identifiable on their own but when combined could become personally identifiable;

n) **Non-Personal Data** means data, including data derived from personal information, that has been generated, modified, or anonymized so that it does not identify any individual, and includes synthetic data and any other type of non-personal data identified in the Regulations;

o) **Personal Information** means recorded information about an identifiable individual, including:

   i. the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent;

   ii. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;

iii. the individual's age, gender identity, sex, sexual orientation, marital status or family status;

iv. an identifying number, symbol or other particular assigned to the individual;

v. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;

vi. information about the individual's health and health care history, including information about the individual's physical or mental health;

vii. information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;

viii. anyone else's opinions about the individual;

ix. the individual's personal views or opinions, except if they are about someone else;

p) **Personal Information Bank or PIB** means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. A PIB allows individuals to know the type of personal information The City may have about them, how it is used, and The City's authority for the collection;

q) **Privacy Incident** means an actual or suspected loss of, or unauthorized access to, use or disclosure of personal information or data derived from personal information;

r) **Privacy Impact Assessment or PIA** means an analytical process to help identify and address potential privacy risks with respect to a new, or substantial change to an existing administrative practice, program, project or service that will involve the collection, use or disclosure of personal information or data derived from personal information;

s) **Privacy Management Program or PMP** means a privacy management program established and implemented under *POPA*;

t) **Privacy Officer** means the person designated or identified to ensure The City's compliance with *POPA*;

u) **Record** means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio, or other medium, but does not include any software or other mechanism used to store or produce the record;

v) **RROSH** means real risk of significant harm; and

w) **Synthetic Data** means artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set.

7. ASSOCIATED GOVERNANCE

7.1 This Administration policy is established in accordance with:

a) The *Municipal Government Act,* RSA 2000, c M-26, s 210, which describes the responsibility of the Chief Administrative Officer to implement the policies and programs of the municipality;

b) The *Access to Information Act*, SA 2024, c A-1.4;

c) The *Protection of Privacy Act*, SA 2024, c P-28.5; and

d) Bylaw 73M94, *City Clerk's Bylaw*, as amended.

8. HISTORY

Action	Date	Approval	Description
Clerical Correction	2026 Jun 01	Leader, Governance and Policy	Updated to current template and formatting, including edits to punctuation and legislative citations.
Amendment	2026 May 11	ELT2026-0380	Updated all sections to align with current legislation and its implementation.
Amendment	2025 Sep 29	ELT2025-0842	Updated all sections to align with new legislative direction. *Freedom of Information and Protection of Privacy Act ("FOIP Act")* replaced by *Access to Information Act ("ATIA")* and the *Protection of Privacy Act ("POPA")*. Effective date October 13, 2025.
New Policy	2023 Dec 18	ELT 2023-1275	Approved December 18, 2023 with an effective date of February 1, 2024. Supercedes GN-022 Privacy Impact Assessment policy.

APPENDIX 1 – PRIVACY INCIDENT RESPONSE PROTOCOL

PURPOSE

This Privacy Incident Response Protocol ("Protocol") outlines the steps that must be followed by all employees when a suspected or actual incident of privacy occurs. The Protocol allows The City to identify, manage and respond to privacy incidents. The purpose of this Protocol is to:

a) Identify roles and responsibilities in responding to a privacy incident; and
b) Establish steps to be followed when responding to a privacy incident.

WHAT IS A PRIVACY INCIDENT?

A privacy incident means a loss of, or unauthorized access to, use or disclosure of personal information. The City's definition of privacy incident is aligned with that of the Office of the Information and Privacy Commissioner ("OIPC") of Alberta.

This would include any event that results in personal information, data derived from personal information in the custody or under the control of The City being collected, accessed, used, copied, modified, disclosed, or disposed of in an unauthorized manner, either deliberately or inadvertently.

KEY STEPS IN RESPONDING TO PRIVACY INCIDENTS

Initiate steps 1 through 3 as soon as a suspected or actual privacy incident has been identified. The Privacy Officer is accountable for all privacy incident activities.

1. Report

1.1. A suspected or actual privacy incident should immediately be reported by any employee to the Privacy Officer.
1.2. Employees can report a privacy incident using the internal *Privacy Incident Report (Internal)* form available on myCity.
1.3. The public can fill out a *Privacy Incident Report (External)* form available on Calgary.ca.

2. Contain

2.1. Identify the scope of the privacy incident and contain it.
2.2. The affected business unit(s) will take and document immediate steps to contain the privacy incident and to secure the related records or information systems to prevent any further privacy incident from occurring. Containment should occur as soon as possible and assistance may be sought from the Privacy Officer. Corporate Security and Information Technology may be engaged to assist with containment. Examples of containment activities include:

- Stopping the unauthorized practice;
- Recovering records;
- Shutting down the information system(s) that may have been breached;
- Revoking or changing computer access codes or correcting weaknesses in physical security; and
- Calling an unintended recipient to request written confirmation of the destruction of a document received in error.

2.3. Employees should be mindful not to destroy evidence that may be valuable in determining the cause and extent of the privacy incident, or that will allow The City to take appropriate corrective action.
2.4. The affected business unit(s) where the privacy incident occurred, should notify Calgary Police Service if the privacy incident involves theft or other criminal activity.

3. Investigate and Evaluation of Risk

3.1. The Privacy Officer will assign resources to investigate with the involvement of other parties, as necessary, and complete the following:
- Identify and analyze the events that led to the privacy incident;
- Obtain all relevant evidence;
- Document the privacy incident and containment activities;
- Inventory all personal information that was subject to the incident and determine the number of affected individuals;
- Determine the level of risk and level of harm; and
- Recommend a Privacy Incident Response Team, where required.

3.2. The Privacy Officer will lead an objective investigation and address any real or perceived conflicts of interest. The Privacy Officer will determine and involve appropriate individuals and/or third-party investigative services, as required.
3.3. The Privacy Officer must evaluate whether the incident meets the threshold of a real risk of significant harm ("RROSH") to an individual.
3.4. As all incidents are unique, the Privacy Officer should exercise their judgment on each incident and consider the factors constituting RROSH under the *Ministerial Regulation*.
3.5. If any other relevant factors exist not included in the *Ministerial Regulation*, they should be considered during the evaluation.
3.6. If the privacy incident does not meet the threshold for RROSH, the privacy incident is tracked, responded to appropriately and recommendations are provided to prevent reoccurrence.
3.7. Privacy incident investigations that meet the threshold for RROSH will result in a *Privacy Incident Investigation Report*.

4. Notification

4.1. The outcome of the investigation and RROSH assessment determines whether notification is required under *POPA*.
4.2. If it is determined that the privacy incident meets the threshold for RROSH, the Privacy Officer is required to give notice, without unreasonable delay, to the affected individual(s), the OIPC and the Minister responsible for *POPA*. Prompt notification can help affected individual(s) mitigate the damage by taking steps to protect themselves.
4.3. Written notification occurs as set out in *POPA*.
4.4. The Privacy Officer will inform Human Resources if notification to affected individual(s) include members of a bargaining unit of The City.
4.5. Affected business unit(s) director(s) must assign a point of contact within three days of receiving the request from the Privacy Officer. The assigned point of contact will be identified as The City's contact, to answer questions about the privacy incident, on the Letter of Notification to the affected individual(s).

4.6. If the affected business unit(s) director(s) are unable to agree to an assigned point of contact within three days of receiving the request, the Privacy Officer will inform the Head. The Head will contact the affected Department General Manager(s) to obtain the point of contact.
4.7. Notification to affected individual(s), the OIPC and the Minister responsible for the Act must be in writing and include the information as prescribed in the *Ministerial Regulation*.

Informing City Leadership and City Council

4.8. Where appropriate, City leadership (including Privacy Officer, affected Business Unit Director, the Head, Human Resources/Labour Relations representative, Business Unit Manager, Business Unit Director, and Department General Manager) will be provided information related to privacy incidents in order to support:
- The response activities;
- The implementation of recommendations; and
- Monitor and follow-up actions to prevent future privacy incidents.

4.9. Responsibilities related to informing and communicating privacy incidents to City leadership and City Council are set out below and in the Privacy Incident Response Procedure.

Individual Informing	**Individual/Group to be Informed**	**When to Inform – Privacy Incidents**
Leader, Access to Information and Investigations	Privacy Officer	All incidents
Privacy Officer	Affected Business Unit Director	Real risk of significant harm assessment – This is initially based on information supplied in the *Privacy Incident Report Form*. Any change to the assessment through the investigation process will be communicated. • Incidents that *may* require notification to affected individuals; and • Incidents that *may* impact the financial, legal or reputational interests of The City. **Will require assignment of point of contact in affected business unit to address questions from affected individual(s).*
	Head of the Local Public Body	• Incidents requiring notification to affected individual(s); • Incidents requiring notification to OIPC and the Minister; • Incidents requiring notification to third-party service providers; and • Incidents impacting the financial, legal or reputational interests of The City.

Individual Informing	Individual/Group to be Informed	When to Inform – Privacy Incidents
	Human Resource/ Labour Relations representative	Incidents requiring notification to affected individual(s) who are members of a bargaining unit of The City.
Business Unit SME	Business Unit Manager/ Business Unit Director	All incidents impacting their area of responsibility.
Business Unit Director	Department General Manager	• Incidents that require escalation to the Head for a point of contact; and • All incidents impacting their area of responsibility.
Department General Manager	Executive Leadership Team	Incidents significantly impacting the financial, legal or reputational interests of The City.
	City Council	

5. Prevent

5.1. Once the immediate steps have been taken to mitigate the risks associated with the privacy incident and notification has been completed (if required), the Privacy Officer and/or the Privacy Incident Response Team will develop prevention strategies to mitigate against similar future privacy incidents.

5.2. Mitigation and prevention strategies should reflect the significance of the privacy incident and whether it was a systemic or isolated event. Strategies may include a review of:

- Physical safeguards (i.e. locks, alarms, security monitoring);
- Technical safeguards (i.e. restricting access, encryption on portable devices); and

5.3. Administrative safeguards (i.e. policies, contractual clauses).

6. Follow-up

6.1. The City tracks all privacy incidents across the organization and uses the information to identify trends in the types of privacy incidents occurring. This information can help identify underlying patterns with respect to personal information and data derived from personal information handling practices and may help prevent future privacy incidents.

6.2. The Privacy Officer will follow-up with the affected business unit(s) on the implementation of recommendations.

7. Privacy Incident Response Team

7.1. Depending on the circumstances of the privacy incident, a Privacy Incident Response Team may be established by the Privacy Officer to respond to a privacy incident. Activities may include carrying out containment and assisting with notification to affected individual(s) to minimize any current, ongoing, or future privacy risks.

7.2. Membership of the Privacy Incident Response Team is determined by the Privacy Officer and varies depending on the context of the privacy incident. Where appropriate, the affected business unit(s) may identify subject matter experts as resources to support the Privacy Incident Response Team.

7.3. The Privacy Incident Response Team may include representation from the following:

Team Member	Role
Privacy Officer	Leads all activities and decisions by the Privacy Incident Response Team, including escalation. Manages the privacy incident response activities to contain, investigate, evaluate, document and make recommendations to mitigate future privacy incidents.
Law	Provides an assessment of The City's legal position and legal advice pertaining to the privacy incident. This may include a review of legal, regulatory and contractual obligations. Reviews external communications to ensure that liability risk is managed.
Information Technology	Provides information system(s) and technology analysis related to privacy incident. Leads the containment activities as it relates to information systems and technologies.
Corporate Security	Provides infrastructure and information asset security analysis related to the privacy incident. Leads security operations, monitoring, and response activities including cybersecurity incidents.
Human Resources / Labour Relations	Provides personnel management and labour relations guidance related to the privacy incident. Leads the personnel management and labour relations activities including liaising with bargaining unit representatives, where required.
Issues Management Office	Provides a communication channel to inform the City Administrator's Office related to high-profile privacy incidents. Informs the Issues Management Program, where required.
Affected Business Unit(s) Customer Service and Communications	Provides support in the development of a communications plan, with tactics, timelines, and key messages for the purpose of preserving The City's reputation, and trust with employees and the public.
Affected Business Unit(s) Subject Matter Expert(s) (SME)	Provides accurate incident details related to the privacy incident. Ensures that the business unit perspective is considered.

7.4. The *Privacy Incident Response Procedure* will include step-by-step instructions to help the Privacy Incident Response Team carry out its responsibilities.

8. Roles and Responsibilities

Individuals	Roles	Responsibilities
All Employees	Employees need to be alert to the potential for personal information to be compromised, play a role in identifying,	• Report privacy incidents to their business unit APPA and supervisor and/or Privacy Officer; • Notify Calgary Police Service if the privacy incident involves theft or other criminal activity;

Individuals	Roles	Responsibilities
	notifying, and containing a privacy incident.	• Immediately undertake containment efforts; and • Assist with privacy incident investigations as required, including making factual corrections to privacy incident information.
APPAs and Alternates	APPAs and Alternates, in consultation with the Privacy Officer, assist their business unit with privacy incident response.	• Assist in reporting, containing, and preventing suspected or actual privacy incidents; • Assist with the collection and preservation of evidence and gathering of facts related to the privacy incident; and • Aid with implementation of recommended mitigations.
Privacy Officer and Access to Information and Investigations	The Privacy Officer is accountable for The City's response to a privacy incident by ensuring that all key steps of the *Privacy Incident Response Protocol* are implemented. The Privacy Officer must address escalation decisions in a timely manner and determines the need to assemble a Privacy Incident Response Team. Access to Information and Investigations manages the response activities to a privacy incident. Response to a privacy incident may include working collaboratively with affected business unit(s) to contain, investigate, evaluate, document and make recommendations to mitigate future privacy risks.	• Intake and validate Privacy Incident Report Form information; • Investigate all suspected and actual privacy incidents; • Direct privacy incident response activities across affected business unit(s); • Support containment of privacy incidents; • Conduct interviews; • Coordinate the collection of evidence and gathering of facts related to the privacy incident, and amend such information for accuracy, when required; • Investigate and evaluate the privacy incident and conduct a real risk of significant harm assessment; • Assemble and lead the Privacy Incident Response Team, when warranted; • Act as decision maker to involve third-party investigative services, as required; • Inform the Head if escalation required for a point of contact for inclusion on the Letter of Notification to address questions from affected individual(s); • Make escalation decisions related to privacy incidents; • Issue a Privacy Incident Investigation Report; • Notify affected individual(s), the OIPC and the Minister, as required;

Individuals	Roles	Responsibilities
		• Inform Human Resources if notification to affected individual(s) includes members of a bargaining unit of The City; • Work with the OIPC, as required; • Issue recommendations to mitigate privacy incidents and follow-up on implementation of recommendations with affected business unit(s); • Close privacy incident response and debrief the Privacy Incident Response Team; • Collect, monitor, and assess all privacy incidents and identify trends and opportunities to prevent future privacy incidents; • Conduct annual tabletop exercises with the Privacy Incident Response Team; and • Ensure Privacy Incident Response Team members are trained and in a state of readiness.
Business Unit Subject Matter Expert ("SME")	Business unit SMEs are individuals who are familiar with the privacy incident details. This individual supports the accuracy of incident documentation and the advancement of activities to close a privacy incident. The business unit SME plays a central role in triggering internal communications to City leadership and City Council.	• Review and fact-check *Draft Privacy Incident Investigation Report;* • Inform the Head if escalation required for a point of contact for inclusion on the *Letter of Notification* to address questions from affected individual(s); • Consult with the business unit Director to assign a point of contact within 3 days of receiving a request from the Privacy Officer. This person will address questions from affected individual(s); and • Inform business unit leadership on the facts relevant to the privacy incident.
Business Unit Manager	Business unit(s) work collaboratively with the Privacy Officer to execute the key steps to responding to a privacy incident. Affected business unit(s) have a role in mitigating recurring risks by implementing recommendations	• Develop and implement a communication plan, as required; • Implement recommendations to mitigate privacy incident; • Consult Human Resources / Labour Relations on personnel management actions, as required; and • Inform and communicate with the Business Unit Director, as required.

Individuals	Roles	Responsibilities
Business Unit Director	The business unit Director plays a central role in ensuring City leadership is aware of the privacy incident.	• Consult Human Resources / Labour Relations on personnel management actions, as required; • Inform and communicate with the department General Manager, as required; and • Assign a point of contact for inclusion on the *Letter of Notification* to address questions from affected individual(s).
Department General Manager	The department General Manager plays a central role in ensuring the Executive Leadership Team and City Council are aware of the privacy incidents that may cause financial, legal or reputational damage to their respective departments.	• Inform and communicate with the Executive Leadership Team and City Council, as required; and • Assign a point of contact for inclusion on the Letter of Notification to address questions from affected individual(s), if required by the Head.
Head of the Local Public Body	Foster public trust and confidence in The City.	• Maintain overall accountability for The City's PMP; and • Inform the affected department General Manager(s) if escalation is required to assign a point of contact for inclusion on the *Letter of Notification* to address.
Privacy Incident Response Team	Supports timely response to more complex privacy incidents.	• Assess, scope, and contain privacy incident; • Mitigate privacy risks; and • Serve as a resource for affected business unit(s). See table in Section 7 above for further details.