Administration Policy

Title: **Protection of Privacy**
Effective Date: **2025 October 13**
Responsible Business Unit **City Clerk's Office**

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, and the *Protection of Privacy Act* (*"POPA"*), SA 2024, Chapter P-28.5, and *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;

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

d) Ensure accountability within The City in making reasonable efforts to provide access to personal information 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 to manage suspected or actual privacy incidents.

2. APPLICABILITY

2.1 This Administration policy applies to:

a) All employees; and

b) All records containing personal information or identifiable through the mosaic effect, 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

3.1 Collection of Personal Information and Notice

a) The City will only collect the 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 of the purpose, the legal authority for the collection, and the contact information of an individual who can answer questions about the collection, and The City's intent, if any, to input the information into an automated system to generate content or make decisions, recommendations or predictions, subject to exceptions under *POPA*.

d) The City is committed to providing a website that respects our visitor's 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 *ATIA and POPA*.

c) The City may only disclose personal information as permitted under *ATIA and POPA*.

d) Access to personal information will be granted in accordance with the *Access and Sharing Standard*.

3.3 Sale of Personal Information

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

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) In the event that an individual believes any of the personal information in the custody or under the control of The City is incorrect, incomplete, or otherwise inaccurate, the individual to whom the personal information relates to may request that it be corrected.

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*.

3.6 Protection of Personal Information

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.

b) The City protects personal information 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.

3.7 Privacy Impact Assessment ("PIA")

a) The City will prepare a PIA 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, as prescribed in *POPA* and the *Ministerial Regulation*.

b) All PIAs will provide a level of detail commensurate with the complexity of the practice, program, project or service the PIA relates to.

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.*

3.8 Privacy Incident Response

a) The City will investigate all privacy-related incidents, including actual and suspected incidents of privacy, and may respond to any privacy-related incident.

b) An investigation is triggered by the submission of a *Privacy Incident Report Form*, through the direction of the Office of the Information and Privacy Commissioner or the Access and Privacy Coordinator.

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

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

4. ROLES AND RESPONSIBILITIES

4.1 Employees are responsible for:

a) Participating in access and privacy training to understand appropriate collection, use, protection, management, disclosure, correction, and disposition of personal information as required by their job duties and responsibilities;

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

c) Implementing reasonable safeguards to protect personal information;

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

f) Reporting any Privacy Incidents to the Access and Privacy Coordinator, and limiting the scope and impact of any privacy incident when possible;

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

h) 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.

4.2 Access and Privacy Program Administrators ("APPA") and Alternates are responsible for:

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

b) Seeking guidance from the Access and Privacy Coordinator regarding new or complex situations involving personal information;

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 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*;

e) Facilitating the completion and maintenance of business unit PIAs;

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

g) Supporting their business unit to protect personal information, report any suspected or actual privacy incidents, helping with audits and privacy incident investigations, and assisting with implementation of corrective actions; and

h) Conducting regular reviews to ensure compliance with *the Protection of Privacy Administration Policy*, including reporting noncompliance concerns to the director or Access and Privacy Coordinator 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:

i. to serve as point of contact for the Access and Privacy Coordinator to ensure that access to information requests are processed effectively;
ii. to ensure that information that can be routinely disclosed is identified; and,
iii. to ensure that privacy protection measures are implemented.

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

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

4.4 Head of the Local Public Body is responsible for:

a) Protecting personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use,

disclosure or destruction as set out in section 10(1) of *POPA;*

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

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

4.5 Access and Privacy Coordinator is responsible for:

a) The overall development, implementation, and management of access to information and protection of personal information within The City;

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

c) Communicating with the Office of the Information and Privacy Commissioner of Alberta, including coordinating any negotiations, mediations, inquiries, and investigations on behalf of The City;

d) 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;

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

f) 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 and any associated standards and procedures 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. 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 to Information Request** means an application under *ATIA* for access to records for general or personal information in the custody or under the control of The City;

b) **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;

c) **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;

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

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

f) **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;

g) **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 section 1(h) of *POPA;*

h) **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 Privacy Management Program;

i) **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****;*

j) **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;

k) **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; and,

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

l) **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;

m) **Privacy Incident** means a loss of, or unauthorized access to, use or disclosure of personal information;

n) **Privacy Impact Assessment or "PIA"** means an analytical process to help identify and address potential privacy 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; and

o) **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.

7. ASSOCIATED GOVERNANCE

7.1 This Administration policy is established in accordance with:

a) *Access to Information Act*, SA 2024, Chapter A-1.4;

b) *Protection of Privacy Act*, SA 2024, Chapter P-28.5*, Protection of Privacy (Ministerial) Regulation*, AR 143/2025 and *Protection of Privacy Regulation*, AR 132/2025; and

c) *The City Clerk's Bylaw*, 73M94 as amended by Bylaw 26M97.

8. HISTORY

Action	Date	Approval	Description
Amendment	2025 September 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 December 18	ELT 2023-1275	Approved December 18, 2023 with an effective date of February 1, 2024. Supercedes GN-022 Privacy Impact Assessment.

SCHEDULE 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 breach 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 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 Access and Privacy Coordinator is accountable for all privacy incident activities.

1. Report

A suspected or actual privacy incident should immediately be reported by any employee to the Access and Privacy Coordinator.

1.1 Employees can report a privacy incident using the internal *Privacy Incident Report Form (Internal)* available on myCity.

1.2 The public can fill out a *Privacy Incident Report Form (External)* available on Calgary.ca.

2. Contain

Identify the scope of the privacy incident and contain it.

2.1 The Access and Privacy Coordinator, with 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. 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.

2.2 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.

2.3 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 Evaluate

Once the privacy incident is contained:

3.1 The Access and Privacy Coordinator 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 real risk of significant harm; and,
- Recommend a Privacy Incident Response Team, where required.

3.2 The Access and Privacy Coordinator will lead an objective investigation and address any real or perceived conflicts of interest. The Access and Privacy Coordinator will determine and involve appropriate individuals and/or third-party investigative services, as required.

3.3 All privacy incident investigations result in a *Letter of Findings*.

4. Notify

<u>Notifying Affected Individuals</u>

4.1 The Access and Privacy Coordinator will determine whether notification is required to be given to the affected individual(s), the OIPC and the Minister. In making the determination, the Access and Privacy Coordinator will consult and collaborate with the affected business unit(s).

4.2 Notification to affected individuals(s) is based on whether the privacy incident creates

a real risk of significant harm to an individual. Prompt notification can help affected individual(s) mitigate the damage by taking steps to protect themselves.

4.3 Notification to affected individual(s) occurs directly unless direct notification could cause more harm, is cost prohibitive or contact information is not available. In such instances, indirect notification may occur.

4.4 The Access and Privacy Coordinator will inform Human Resources if notification to affected individuals 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 Access and Privacy Coordinator. 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 Access and Privacy Coordinator will inform the Head of the Local Public Body. The Head of the Local Public Body will contact the affected Department General Manager(s) to obtain the point of contact.

4.7 Notifications to individuals should include the following information:

- Date of the privacy incident and the date the incident was discovered;
- Description of the privacy incident;
- General description of information lost, accessed, used or disclosed without authorization;
- Steps taken so far to mitigate the harm or risk of harm;
- Steps the affected individual can take to further mitigate the risk of harm;
- Contact information of an individual within the affected business unit who can answer questions or provide further information;
- That individuals have a right to complain to the OIPC; and
- Any other relevant information.

<u>Informing City Leadership and City Council</u>

4.8 Where appropriate, City leadership (including Access and Privacy Coordinator, affected Business Unit Director, Head of the Local Public Body, 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	Access and Privacy Coordinator	All incidents
Access and Privacy Coordinator	Affected Business Unit Director	Initial risk and harms assessment – This is based on information supplied in the *Privacy Incident Report Form.* • Incidents that *may* require notification to affected individuals; and, • Incidents that *may* impact the financial, legal or reputation of The City. *Post risk and harms assessment – This is based on the evidence obtained through the investigation. • Incidents requiring notification to affected individual(s); and, • Incidents impacting the financial, legal or reputation 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 reputation of The City.
and Privacy Coordinator	Human Resources/Labour Relations representative	Post risk and harms assessment – This is based on the evidence obtained through the investigation. • Incidents requiring notification to affect individuals 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.

Individual Informing	Individual/Group to be Informed	When to Inform – Privacy Breaches Incidents
Business Unit Director	Department General Manager	• Incidents that require escalation to the Head of the Local Public Body for a point of contact; and, • All incidents impacting their area of responsibility.
Department General Manager	Executive Leadership Team City Council	Incidents impacting the financial, legal or reputation of The City.

5. Prevent

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

5.1 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 (locks, alarms, security monitoring);
- Technical safeguards (restricting access, encryption on portable devices); and
- Administrative safeguards (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 handling practices and may help prevent future privacy incidents.

6.2 Access to Information and Investigations section 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 Access and Privacy Coordinator to respond to a privacy incident. Activities may include carrying out containment and assisting with notification to affected individuals to minimize any current, ongoing, or future privacy risks.

7.2 Membership of the Privacy Incident Response Team is determined by the

Access and Privacy Coordinator 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.

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

Team Member	Role
Access and Privacy Coordinator	Leads all activities and decisions by the Privacy Incident Response Team, including escalation and notification decisions.
Access to Information and Investigations	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 systems and technology analysis related to the privacy incident. Leads the containment activities as it relates to information systems and technologies.

Team Member	Role
Corporate Security	Provides infrastructure and information asset security analysis related to the privacy incident. Leads the security operations, monitoring, and response activities including cyber security 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.

7.3 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, notifying, and containing a privacy incident.	• Report suspected or actual privacy breaches to their business unit APPA and supervisor and/or Access and Privacy Coordinator; • Notify Calgary Police Service if the privacy incident involves theft or other criminal activity; • 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 Access and Privacy Coordinator, assists 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.
Access and Privacy Coordinator and Access to Information and Investigations	The Access and Privacy Coordinator 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 Access and Privacy Coordinator must address escalation decisions in a timely manner, confirms notification requirements, 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	• 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 incident; • Conduct interviews; • Coordinate the collection of evidence and gathering of facts related to the privacy incident, and amending such information for accuracy, when required; • Investigate and evaluate the privacy incidents and conduct a risk and harms assessment;

Individuals	Roles	Responsibilities
	privacy incident may include working collaboratively with affected business unit(s) to contain, investigate, evaluate, document and make recommendations to mitigate future privacy risks.	• 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 of the Local Public Body 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 *Letter of Findings*; • Determine whether to provide notification upon review of incident; • Notify affected individual(s), as required; • Inform Human Resources if notification to affected individual(s) include members of a bargaining unit of The City; • Notify and work with the OIPC, as required; • Notify the Minister, as required; • Issue recommendations to mitigate privacy incidents and follow-up on implementation of recommendations with affected business unit(s);

Individuals	Roles	Responsibilities
		• 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 Letter of Findings*; • Consult with the Business Unit Director to assign a point of contact within 3 days of receiving a request from the Access and Privacy Coordinator. 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 Access and Privacy Coordinator to execute the key steps to responding to a privacy incident. Affected business unit(s) have a role in mitigating recurring risks	• Develop and implement a communication plan, as required; • Implement recommendations to mitigate privacy incidents; • Consult Human Resources/Labour Relations on

Individuals	Roles	Responsibilities
	by implementing recommendations.	personnel management actions, as required; and • Inform and communicate with the Business Unit Director, as required.
Business Unit Director	The Business Unit Director plays a central role in ensuring City leadership is aware of privacy incidents.	• 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 of the Local Public Body.
Head of the Local Public Body	Foster public trust and confidence in The City.	• Maintain overall accountability for The City's Privacy Management Program; 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

Individuals	Roles	Responsibilities
		questions from affected individual(s).
Privacy Incident Response Team	Supports timely response to more complex privacy incidents.	• Assess, scope, and contain privacy incident; • Mitigate privacy risks; • Resource for affected business unit(s); and • See table in Section 7, above for further details.