Administration Policy

Policy Title:	**Protection of Privacy**
Adopted by:	**Executive Leadership Team**
Effective Date:	**February 01, 2024**
Last Updated:	**December 18, 2023**
Responsible Service(s)	**Records Management, Access and Privacy**

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 *Freedom of Information and Protection of* Privacy Act *("FOIP Act")*, RSA 2000, Chapter F-25, as amended;

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 Breach Response Protocol to manage suspected or actual privacy breaches.

2. POLICY STATEMENT

2.1 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 the *FOIP Act*.

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, subject to exceptions under the *FOIP Act*.

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 the *FOIP Act,* and the Privacy Policy of the website.

2.2 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 the *FOIP Act*.

c. The City may only disclose personal information as permitted under the *FOIP Act*.

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

2.3 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 the *FOIP Act*.

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 annotated or corrected.

2.4 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*.

2.5 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.

2.6 Privacy Impact Assessment ("PIA")

a. The City will complete a PIA for any new or modified project, initiative, program, administrative practice or process, or information system, that collect, use, or disclose personal information to:

(i) ensure technical compliance with the *FOIP Act*;
(ii) assess privacy implications to individuals;
(iii) identify and address privacy risks that may arise in the course of implementation and/or operations; and
(iv) provide public confidence.

b. A completed PIA is required before implementation of a project, initiative, program, administrative practice or process, or information system that involves the collection, use, or disclosure of personal information.

2.7 Incident / Privacy Breach Response

a. The City will investigate all privacy-related complaints, including actual and suspected breaches of privacy, and may respond to any privacy-related complaint.

b. An investigation is triggered by the submission of a *Privacy Breach Form*, through the direction of the Office of the Information and Privacy Commissioner or the FOIP 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 breach.

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

3. DEFINITIONS

3.1 In this Administration Policy:

a. **"Access to Information Request"** means an application under the *FOIP Act* 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 breach 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(e) of the *FOIP Act;*

h. **"FOIP Program Administrator" or "FOIP PA" 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 the *FOIP Act;*

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:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status, or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and,
- 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 Breach"** 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 risks before the implementation of a project, initiative, program, administrative practice or process, or information system; and

o. **"Record"** means recorded information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded, or stored in any manner, but does not include software or any mechanism that produces records.

4. APPLICABILITY

4.1 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.

4.2 *This Administration Policy does not apply to*:

a. Elected officials;

b. Calgary Housing Corporation employees; and,

c. Calgary Police Service employees.

4.3 If any provision of this Administration Policy conflicts with any provision of the *FOIP Act*, the provision of the *FOIP Act* prevails.

5. LEGISLATIVE AUTHORITY

5.1 This policy is established in accordance with:

a. Freedom of Information and Protection of Privacy Act, RSA 2000, Chapter F-25, as amended; and

b. The City Clerk's Bylaw, 73M94 as amended by Bylaw 26M97.

6. ROLES AND RESPONSIBILITIES

6.1 *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 the *FOIP Act*;

c. Implementing reasonable safeguards to protect personal information;

d. Participating in PIAs to help identify and address potential privacy risks before the implementation of a project, initiative, program, administrative practice or process, or information system that involves 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 suspected or actual privacy breach to the FOIP Coordinator, and limiting the scope and impact of any privacy breach 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 the *FOIP Act,* if this is practical and expedites public business, when directly requested by the individual whom the personal information relates to.

6.2 *FOIP Program Administrators (PAs) and Alternates are responsible for:*

a. Attending FOIP PA specific training, and in consultation with the FOIP Coordinator, providing corresponding advice and guidance to their business unit regarding compliance with the *FOIP Act*;

b. Seeking guidance from the FOIP 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 breaches, helping with audits and privacy complaint 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 FOIP Coordinator when issues arise.

6.3 *Business Unit Directors are responsible for:*

a. Ensuring the business unit has a FOIP Program Administrator ("PA") and Alternate appointed for their business unit:

(i) to serve as point of contact for the FOIP 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*.

6.4 *The City Clerk, as Head of the local public body (The City), 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 38 of the *FOIP Act;*

b. All obligations of the Head under the *FOIP Act* that relate to The City; and

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

6.5 *The FOIP 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 the *FOIP Act*;

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 Part 2 of the *FOIP Act* regarding the collection, use, disclosure, accuracy, retention, and safeguards of personal information;

e. Leading The City's training on the *FOIP Act*, policies, procedures, and tools; and

f. Leading The City's privacy breach response and Privacy Breach Response Team, when required.

7. CONSEQUENCES OF NON-COMPLIANCE

7.1 Employees who fail to adhere to this Administration Policy and any associated standards and procedures may result in disciplinary action in accordance with either the *Labour Relations Policy* or *Exempt Staff Policy*. Failure to comply with the duties imposed by the *FOIP Act* or otherwise acting in contravention of the legislation may lead to penalties or offences under the *FOIP Act*.

8. HISTORY

Policy Action	Date	Report Number	Description
New Policy	December 18, 2023	ELT 2023-1275	Approved December 18, 2023 with an effective date of February 1, 2024. Supercedes GN-022 Privacy Impact Assessment

APPENDIX 1 – PRIVACY BREACH RESPONSE PROTOCOL

PURPOSE

This Privacy Breach 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 breaches. The purpose of this Protocol is to:

a) Identify roles and responsibilities in responding to a privacy breach; and

b) Establish steps to be followed when responding to a privacy breach.

WHAT IS A PRIVACY BREACH?

A privacy breach means a loss of, or unauthorized access to, use or disclosure of personal information. The City's definition of privacy breach 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 BREACHES

Initiate steps 1 through 3 as soon as a suspected or actual privacy breach has been identified. The FOIP Coordinator is accountable for all privacy breach activities.

1. Report

A suspected or actual privacy breach should immediately be reported by any employee to the FOIP Coordinator.

1.1 Employees can report a privacy breach using the internal *Privacy Breach Form* available on myCity.

1.2 The public can fill out a *Privacy Complaint Form* available on Calgary.ca.

2. Contain

Identify the scope of the privacy breach and contain it.

2.1 The FOIP Coordinator, with the affected business unit(s) will take and document immediate steps to contain the privacy breach and to secure the related records or information systems to prevent any further privacy breach 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 breach, or that will allow The City to take appropriate corrective action.

2.3 Affected business unit(s) where the privacy breach incident occurred, should notify Calgary Police Service if the privacy breach involves theft or other criminal activity.

3. Investigate and Evaluate

Once the privacy breach is contained:

3.1 The FOIP 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 breach;
- Obtain all relevant evidence;
- Document the privacy breach and containment activities;
- Inventory all personal information that was subject to the breach and determine the number of affected individuals;

- Determine the level of risk and level of harm; and,
- Recommend a Privacy Breach Response Team, where required.

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

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

4. Notify

Notifying Affected Individuals

4.1 The FOIP Coordinator will determine whether notification will be given to the affected individual(s) and/or the OIPC. In making the determination, the FOIP Coordinator will consult and collaborate with the affected business unit(s).

4.2 Notification to affected individuals(s) is based on whether the privacy breach creates a real risk of significant harm to an individual. Prompt notification can help 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 FOIP 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 FOIP Coordinator. The assigned point of contact will be identified as The City's contact, to answer questions about the privacy breach, 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 FOIP Coordinator will inform the FOIP Head. The FOIP Head 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 breach;
- Description of the privacy breach;
- 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;
- Next steps planned and any long term plans to prevent future breaches;

- Contact information of an individual within the affected business unit who can answer questions or provide further information; and
- That individuals have a right to complain to the OIPC.

Informing City Leadership and City Council

4.8 Where appropriate, City leadership (including FOIP Coordinator, affected Business Unit Director, FOIP Head/City Clerk, Human Resources/Labour Relations representative, Business Unit Manager, Business Unit Director, and Department General Manager) will be provided information related to privacy breach incidents in order to support:

- The response activities;
- The implementation of recommendations; and
- Monitor and follow-up actions to prevent future privacy breaches.

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

Individual Informing	**Individual/Group to be Informed**	**When to Inform – Privacy Breach Incidents**
Leader, Access to Information and Investigations	FOIP Coordinator	All incidents
FOIP Coordinator	Affected Business Unit Director	Initial risk and harms assessment – This is based on information supplied in the *Privacy Breach 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).*

Individual Informing	Individual/Group to be Informed	When to Inform – Privacy Breach Incidents
	FOIP Head/City Clerk	• Incidents requiring notification to affected individual(s); • Incidents requiring notification to OIPC; • Incidents requiring notification to third-party service providers; and, • Incidents impacting the financial, legal or reputation of The City.
FOIP Coordinator	Human Resource/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.
Business Unit Director	Department General Manager	• Incidents that require escalation to the FOIP Head 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 breach and notification has been completed (if required) the FOIP Coordinator and/or the Privacy Breach Response Team will develop prevention strategies to mitigate against similar future privacy breaches.

5.1 Mitigation and prevention strategies should reflect the significance of the privacy breach 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 breaches across the organization and uses the information to identify trends in the types of privacy breaches occurring. This information can help identify underlying patterns with respect to personal information handling practices and may help prevent future privacy breaches.

6.2 Access to Information and Investigations section will follow-up with the affected business unit(s) on the implementation of recommendations.

7. PRIVACY BREACH RESPONSE TEAM

7.1 Depending on the circumstances of the privacy breach, a Privacy Breach Response Team may be established by the FOIP Coordinator to respond to a privacy breach. 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 Breach Response Team is determined by the FOIP Coordinator and varies depending on the context of the privacy breach. Where appropriate, the affected business unit(s) may identify subject matter experts as resources to support the Privacy Breach Response Team.

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

Team Member	Role
FOIP Coordinator	Leads all activities and decisions by the Privacy Breach Response Team, including escalation and notification decisions.
Access to Information and Investigations	Manages the privacy breach response activities to contain, investigate, evaluate, document and make recommendations to mitigate future privacy breaches.
Law	Provides an assessment of The City's legal position and legal advice pertaining to the privacy breach. 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 breach. 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 breach. 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 breach. 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 breach 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 breach. Ensures that the business unit perspective is considered.

7.3 The *Privacy Breach Response Procedure* will include step-by-step instructions to help the Privacy Breach 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 breach.	• Report suspected or actual privacy breaches to their business unit FOIP PA and supervisor and/or FOIP Coordinator; • Notify Calgary Police Service if the privacy breach involves theft or other criminal activity; • Immediately undertake containment efforts; and

Individuals	Roles	Responsibilities
		• Assist with privacy breach investigations as required, including making factual corrections to privacy breach incident information.
FOIP PAs and Alternates	FOIP PAs and Alternates, in consultation with the FOIP Coordinator, assists their business unit with privacy breach response.	• Assist in reporting, containing, and preventing suspected or actual privacy breaches; • Assist with the collection and preservation of evidence and gathering of facts related to the privacy breach incident; and, • Aid with implementation of recommended mitigations.
FOIP Coordinator and Access to Information and Investigations	The FOIP Coordinator is accountable for The City's response to a privacy breach incident by ensuring that all key steps of the *Privacy Breach Response Protocol* are implemented. The FOIP Coordinator must address escalation decisions in a timely manner, confirms notification requirements, and determines the need to assemble a Privacy Breach Response Team. Access to Information and Investigations manages the response activities to a privacy breach incident. Response to a	• Intake and validate *Privacy Breach Form* information; • Investigate all suspected and actual privacy breaches; • Direct privacy breach response activities across affected business unit(s); • Support containment of privacy breaches; • Conduct interviews; • Coordinate the collection of evidence and gathering of facts related to the privacy breach incident, and amending such information for accuracy, when required; • Investigate and evaluate the privacy breach and conduct a risk and harms assessment;

Individuals	Roles	Responsibilities
	privacy breach 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 Breach Response Team, when warranted; • Act as decision maker to involve third-party investigative services, as required; • Inform the FOIP 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 breach 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; • Issue recommendations to mitigate privacy breaches and follow-up on implementation of recommendations with affected business unit(s);

Individuals	Roles	Responsibilities
		• Close privacy breach incident response and debrief the Privacy Breach Response Team; • Collect, monitor, and assess all privacy breaches and identify trends and opportunities to prevent future privacy breaches; • Conduct annual tabletop exercises with the Privacy Breach Response Team; and • Ensure Privacy Breach 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 breach incident details. This individual supports the accuracy of incident documentation and the advancement of activities to close a privacy breach 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 FOIP Coordinator. This person will address questions from affected individual(s); and • Inform business unit leadership on the facts relevant to the privacy breach incident.
Business Unit Manager	Business unit(s) work collaboratively with the FOIP Coordinator to execute the key steps to responding to a privacy breach. Affected business unit(s) have a role in mitigating recurring risks	• Develop and implement a communication plan, as required; • Implement recommendations to mitigate privacy breaches; • 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 breach 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 breach 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 FOIP Head.
FOIP Head	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 Breach Response Team	Supports timely response to more complex privacy breach incidents.	• Assess, scope, and contain privacy breach; • Mitigate privacy risks; • Resource for affected business unit(s); and • See table in Section 7, above for further details.