The City of Calgary

Privacy Management Program

Approved by The City of Calgary Acting Head

Effective June 11, 2026

City of Calgary
Privacy Management Program
Overview

The *Protection of Privacy Act* (POPA) requires public bodies in Alberta to have a Privacy Management Program. This program helps The City of Calgary (The City) manage personal information with care and reduce privacy risks.

A clear and accessible Privacy Management Program helps The City protect personal information, respond to privacy risks, and support public trust. It also helps us meet our legal responsibilities.

Governance and accountability

Protection of Privacy Administration Policy

The City is committed to protecting your personal information. The City's Protection of Privacy Administration Policy lays out the principles, responsibilities, and practices that guide how The City collects, manages, uses, and protects personal information, data derived from personal information, and non-personal data.

The Policy also includes a Privacy Incident Response Protocol (Appendix 1). This identifies roles, responsibilities, and specific steps that must be followed by employees in the event of a privacy incident.

Privacy Officer designation

The City has designated the Privacy Officer position to help ensure compliance with POPA.

Position title: Privacy Officer

Department: Law, Legislative Services & Security

Contact: AccessandPrivacy@calgary.ca

The Privacy Officer is responsible for:

- Overseeing and coordinating The City's compliance with POPA and this Privacy Management Program;
- Providing advice to business areas about privacy responsibilities, policies, and procedures;
- Reviewing and approving privacy impact assessments;
- Managing the privacy incident response process;
- Overseeing mandatory privacy awareness training;
- Acting as the main contact with the Privacy Commissioner; and
- Maintaining and regularly reviewing this Privacy Management Program.

City of Calgary
Privacy Management Program
Overview

Who is responsible for privacy?

We all have an important role in upholding the privacy standards set out in the Protection of Privacy Administration Policy and its accompanying standards. The Policy outlines the general responsibilities by the different roles to ensure The City is compliant with POPA.

Privacy Management Program review, assessment and update

This Privacy Management Program is reviewed, assessed and updated from time to time but no less than every two years. The Privacy Officer is responsible for this review.

Public availability of the Privacy Management Program

The City makes this Privacy Management Program available to the public, as required by the *Ministerial Regulation*.

Rights, requests, and complaints

Requests to correct personal information

If you believe personal information The City holds about you is incorrect, you can ask for it to be corrected by filling out the form.

The City has a standard that explains how these requests are received and reviewed under section 7 of POPA.

Incident response

The City has policies and procedures in place to help staff respond to privacy incidents carefully and consistently, as required by section 10(2) of POPA. See page 13 of the Protection of Privacy Policy for further details.

Complaint response

If you have concerns about how The City collected, used, or shared your personal information, you can make a complaint to The City first. This is the first step before asking the Office of the Information and Privacy Commissioner of Alberta (the Commissioner) to review the matter.

To make a complaint, please contact us at AccessandPrivacy@calgary.ca.

We will acknowledge your complaint within two business days. We aim to review and respond within 30 business days of receiving your complaint.

City of Calgary
Privacy Management Program
Overview

If we are unable to resolve your complaint, we will let you know about your right to make a complaint to the Commissioner under section 38 of POPA.

You may also ask the Commissioner to review the matter if you believe your personal information was collected, used, or shared in a way that does not follow POPA.

Data handling and safeguards

Non-personal data

The City is developing documentation on how employees must create, use, and share non-personal data in line with POPA. We also provide guidance and tools to help staff follow these requirements and use good practices when creating non-personal data.

Artificial intelligence, data derived from personal information and data matching

The City's Proactive Monitoring and Safeguards for Information Systems document explains how employees must handle personal information used in artificial intelligence systems, how data derived from personal information may be created, and how non-personal data may be created, in line with POPA.

Automated systems using personal information

The City uses automated systems involving personal information in line with POPA. The Proactive Monitoring and Safeguards for Information Systems explains the safeguards in place to help protect personal information in these systems. Some technical and security details have been removed, as allowed under section 6(4) of the *Ministerial Regulation*, to help protect the security of the information.

Information security classification system

The City maintains an information security classification system that applies to all personal information, data derived from personal information, and non-personal data in the custody or under the control of The City.

Written administrative, technical and physical safeguards

The City's Proactive Monitoring and Safeguards for Information Systems explains the administrative, technical, and physical safeguards in place to help protect personal information, data derived from personal information, and non-personal data. Some

City of Calgary
Privacy Management Program
Overview

technical and security details have been removed, as allowed under section 6(4) of the *Ministerial Regulation*, to help protect the security of the information.

As part of our commitment to secure The City's technology environment and protect The City's data and information the Acceptable Use of City Technology Resources Administration Policy outlines the expectations regarding the use of City technology resources.

Training and awareness

Mandatory employee training

All City employees must complete privacy awareness training.

This training helps employees understand how to protect personal information and meet their responsibilities under POPA. It covers:

- An overview of POPA and what employees are required to do;
- The rules for collecting, using, sharing, and protecting personal information;
- The right to ask for a correction to personal information;
- How to identify and respond to privacy incidents; and
- The City's privacy policy and the roles employees play in protecting personal information.

New employees complete this training by the end of their first calendar year. Employees complete refresher training every year. The training is offered online through the Corporate Learning & Development portal. Human Resources keeps the training records.

Compliance, risk, and assessment

Privacy impact assessment process

The City's Privacy Compliance and Risk Assessment Standard explains when a privacy impact assessment is required and how employees must complete one under section 26(1) of POPA.

Proactive monitoring of information systems

The City proactively monitors information systems that hold personal information, data derived from personal information, and non-personal data. The Proactive Monitoring and Safeguards for Information Systems explains these monitoring activities and the

City of Calgary
Privacy Management Program
Overview

safeguards in place to help protect this information. Some technical and security details have been removed, as allowed under section 6(4) of the *Ministerial Regulation*, to help protect the security of the information.

Consent policies and procedures

The City has a standard that explains how employees must ask for oral, written, or electronic consent before using or sharing personal information, in line with section 2 of the *Protection of Privacy Regulation*.

Supporting documents

Document name
Office consolidation of the Privacy Management Program
Protection of Privacy Policy, including Privacy Incident Response Protocol
Correction of Personal Information Standard
Guide to Creating Non-Personal Data (PDF coming soon)
Record of Creation of Non-Personal Data (PDF coming soon)
Proactive Monitoring and Safeguards for Information Systems
Acceptable Use of City Technology Resources Policy
Information Security Classification Standard
Privacy Compliance and Risk Assessment Standard
Consent to Use or Disclose Personal Information Standard

Administration Policy

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 02	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.

Administration Standard

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

1. PURPOSE

1.1 This Administration standard will be followed when The City of Calgary ("The City") receives a request to correct personal information pursuant to the *Protection of Privacy Act* ("*POPA*") of Alberta.

1.2 Following this standard will result in:

a) Promoting the accuracy and completeness of personal information in the custody or under the control of The City;

b) Consistent and transparent processes being applied for the correction of personal information; and

c) Meeting legislative obligations for responding to requests to correct an individual's personal information, including requests made by an authorized representative.

2. APPLICABILITY

2.1 This Administration standard applies to all City employees except:

a) Calgary Police Services, as a separate public body; and

b) Calgary Housing Corporation, as a separate public body.

2.2 This Administration standard applies to all records in the custody or under the control of The City.

3. STANDARD

3.1 Employees will:

a) Maintain the accuracy and completeness of personal information in The City's custody or control;

b) Correct factual personal information without a formal request under *POPA*, if the information is not an opinion about the individual, including a professional or expert opinion, or an incorrect fact stated in a record of a third party or other public body;

c) Direct requests for correction of personal information to the appropriate business unit area or to the Privacy Officer for guidance and/or processing;

d) Verify the identity of the individual requesting a factual correction, or, where a request is made by a representative, verify both the identity of the individual and the authority of the representative to act on their behalf, before processing the correction request;

e) Verify that all factual correction requests are supported by appropriate and relevant documentation or information to substantiate the requested correction;

f) Make the requested corrections, or, where a correction is not made, apply an annotation or linkage to the request across all systems containing the personal information; and

g) Document the decision.

3.2 Access and Privacy Program Administrators ("APPA") will:

a) Help their respective business units maintain compliance with the Administration standard;

b) Identify public bodies or third parties that received the individual's personal information that was corrected or annotated within the year prior to the request for correction;

c) Assess whether the corrected or annotated personal information is material; and

d) Provide the Privacy Officer with the information needed in a timely manner to complete required notifications to third parties or other public bodies.

3.3 Business Unit Managers will:

a) Ensure business unit implementation of the Administration standard;

b) Authorize the correction of personal information required by the business unit area; and

c) Ensure the APPA is notified of any corrections to personal information made by the business unit area so the Privacy Officer can issue required notifications.

3.4 The Privacy Officer will:

a) Notify public bodies or third parties that received the individual's personal information within the year prior to the request for correction, where the correction or annotation is material;

b) Dispense notification to public bodies or third parties, where the correction or annotation is immaterial, or the individual has provided written consent or agreement that notification is not required; and

c) Ensure the individual receives written notice within 30 business days indicating whether the correction was made, or an annotation or linkage has been added.

4. CONSEQUENCES OF NON-COMPLIANCE

4.1 Employees who fail to adhere to this Administration standard 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.

4.2 In addition to any consequences from The City associated with not adhering to this Administration standard, failure to comply with the duties imposed by *POPA* or otherwise acting in contravention of the legislation may lead to penalties or offences under *POPA*.

5. DEFINITIONS

5.1 In this Administration standard:

a) **Annotation** means a note added to a record indicating the individual's request for correction if no correction is made, and date it was added. An annotation is placed close to the disputed information;

b) **Authorized Representative** means a person who is legally entitled to exercise an individual's rights or powers on the individual's behalf, including a personal representative of a deceased individual, a guardian or trustee, an agent or attorney, or any person with written authorization from the individual to act on the individual's behalf;

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

d) **Correction** means a change to factual personal information to make it accurate or complete;

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

f) **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*;

g) **Factual** means what is actual or based on fact such as age, date of birth, contact information, income information and qualifications;

h) **Linkage** means a mechanism used when a record cannot be directly updated, attaching, connecting the individual's correction request to the original record;

i) **Opinion** means a subjective assessment, evaluation, or professional judgement about an individual. Opinions cannot be corrected but must be annotated or linked with the individual's request for correction;

j) **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.

k) **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 software or any mechanism that produces records.

6. ASSOCIATED GOVERNANCE

6.1 This Administration standard outlines requirements in support of the *Protection of Privacy policy*.

6.2 This Administration standard conforms to the *Protection of Privacy Act* ("*POPA*") and *Protection of Privacy (Ministerial) Regulation* ("*Ministerial Regulation*").

6.3 If any provision of this Administration standard conflicts with any provision of *POPA*, the provision of *POPA* prevails.

7. HISTORY

Action	Date	Approval	Description
New	2026 Jun 01	Head of the Local Public Body	New Standard developed during the review of the Protection of Privacy policy.

Administration Policy

Title:	**Acceptable Use of City Technology Resources**
Effective Date:	**2025 July 28**
Responsible Business Unit:	**Information Technology**

1. PURPOSE

1.1 The purpose of this Administration policy is to:

a) Outline The City of Calgary's ("The City") expectations regarding the secure, responsible, and ethical use of City Technology Resources;

b) Protect The City's interests and reputation; and

c) Ensure the responsible use of taxpayer dollars.

2. APPLICABILITY

2.1 This Administration policy applies to all Employees, Volunteers, or Suppliers that have been authorized to use City Technology Resources; and

2.2 This Administration policy does not apply to those working in the Mayor's Office, the Calgary Police Service, Civic Partners, and City Council and their ward office staff.

3. POLICY STATEMENT

3.1 General Principles for the Use of City Technology Resources

a) All Technology Resources purchased, contracted, and/or managed by The City belong to The City or its licensors;

b) The City's Technology Resources will only be used for the delivery of City services and related business activities;

c) The City's Technology Resources will be used in compliance with all applicable laws or regulations, including, without limitation, those at the federal level, provincial level, and municipal level; those by way of international treaties; those of any foreign jurisdiction with authority; those civil laws in force between vendor and purchaser of Technology Resources; and all City policies; and

d) The Chief Information Technology Officer will have the authority to approve exceptions to this policy.

3.2 Use of City Credentials

a) Technology Resource Users will only access City Technology Resources using their City Credentials;

b) Technology Resources Users will not use or operate under another City Technology Resource User's Credentials or generic / shared account;

c) Technology Resource Users will not share or reveal their Network Account passwords or Multi-Factor Authentication methods;

d) City Credentials will only be used for City business purposes. The use of City Credentials to access or participate in online services unrelated to City business is prohibited without the prior written permission from the Chief Information Technology Officer; and

e) Only City Credentials will be used for City business purposes and linking to City Technology Resources. Personal accounts should not be used on City Technology Resources.

3.3 Safeguarding Assets

a) Technology Resource Users will exercise care to prevent the abuse or theft of The City's Technology Resources. Any City Technology Resources that are suspected of being lost or stolen must be reported to the IT Help Desk immediately;

b) Except for Portable Computing Devices and Mobile Devices, City Technology Resources will not be removed from the corporate workspace without an existing agreement or prior approval from the Technology Resource User's Exempt Supervisor and the Chief Information Technology Officer;

c) Information Technology reserves the right to deny the use of certain devices, peripherals, or software on its network or systems based on security concerns, compatibility issues, or other operational considerations. Technology Resource Users will comply with such decisions promptly and refrain from installing unauthorized software or connecting unauthorized devices to the network. If a device is deemed unacceptable, The City may take appropriate actions, including disabling network access or restricting specific functionalities;

d) Technology Resource Users will ensure that City Technology Resources are kept compliant with updates (e.g. operating system, firmware, security, etc.) and lifecycle replacement schedules. Devices that are not compliant will be deemed inoperable and must be returned to the IT Manager, Operations;

e) Technology Resources Users will not keep duplicate, secondary, or backup devices (e.g. multiple computing devices or multiple Mobile Devices). Any device deemed to be a duplicate, secondary, or backup device by Information Technology will be returned to the IT Manager, Operations or the IT Manager, Innovation & Collaboration;

f) Technology Resource Users using Mobile Devices will ensure their devices are kept compliant with updates (e.g. operating system, security, etc.) and lifecycle replacement schedules and do not pose security risks to The City. Mobile Devices must have Mobile Device management tools installed. Once a Mobile Device is no longer supported by the manufacturer, it will be deemed end-of-life and will need to be replaced. Once a Mobile Device has been replaced, Technology Resource Users will return the old device to Information Technology for proper disposal; and

g) Removable Devices will not be supported as they are not backed up by City technology and they pose significant security risks. Exceptions will need to be approved by the Chief Information Technology Officer. Official records, cardholder Information, personal Information, or any documents with an information security classification of confidential or highly restricted must never be stored on removable media.

3.4 Safeguarding Information

a) The City's Technology Resources will be used in a manner that protects the integrity and accessibility of Information created, received, and/or downloaded from external resources;

b) City Information will only be stored at a City-approved vendor site, on a City network drive, or on a City-approved corporate Cloud Solution (e.g. OneDrive). City Information will not be stored on a technology device's local hard drive (e.g. computer desktop) or transferred to a Technology Resource User's personal email or other non-corporate Cloud Solution. Any Information with an information security classification of unrestricted that needs to be temporarily stored on a technology device's local hard drive (e.g. smartphone) must be transferred to a City-approved storage location and deleted from the device's hard drive at the earliest opportunity;

c) City Information stored at a vendor's location will be protected through contracts and will comply with City policies and guidelines. The City will ensure it has the option to transfer City Information from the vendor site back to The City's technology environment at the end of the contract;

d) Technology Resources Users will use Multi-Factor Authentication to access City Information when working from a non-corporate Workplace and when working with City Technology Resources where Multi-Factor Authentication is configured;

e) Technology Resource Users will not open or access any technology links or attachments that are from unknown sources as they could pose a security risk to The City. Technology Resource Users that have clicked links or opened attachments in a suspicious email must contact the IT Help Desk immediately to report the incident;

f) Software acquisitions (free or purchased), including Cloud Solutions and software subscriptions, will adhere to all procurement policies. A Risk/Value Assessment will be completed for all Cloud Solutions and will be subject to approval by the Chief Information Technology Officer. Access to Cloud Solutions prior to the completion of a Risk/Value Assessment will not be permitted;

g) New or emerging technologies, including, but not limited to, Artificial Intelligence, must be approved by the Chief Information Technology Officer prior to implementation or use; and

h) City Information will not be shared or used for third-party tools (e.g. Artificial Intelligence tools) unless approved by the Chief Information Technology Officer or the Information Technology Management Team.

3.5 Monitoring the Use of Technology Resources

a) The City may monitor, access, investigate, audit, and/or disclose information related to the use of City Technology Resources or use of Credentials to Corporate Security and/or Human Resources for investigative purposes in the event of a suspected breach of this policy;

b) The City may monitor, access, investigate, audit, and/or disclose any Information accessed by or contained on any City Technology Resource to Corporate Security and/or Human Resources at any time without notice for investigative purposes in the event of a suspected breach of this policy. Technology Resource Users shall not have any expectation of privacy as to their Technology Resource use;

c) The City may remove City Technology Resources or access to The City's Technology Resources at any time without notice with the approval of the Chief Information Technology Officer; and

d) The City may remove any Information on any of The City's Technology Resources at any time without notice with the approval of the Chief Information Technology Officer. Corporate Information on non-corporate assets may also be removed. Information or records that need to be retained due to business, legal, or audit needs will be moved to a secure network storage location determined by the Chief Information Technology Officer.

3.6 Personally Owned Technology Resources

a) The City will not provide funding or technological support for personally-owned Technology Resources, including, but not limited to, personal Mobile Devices, Mobile Device services, home Internet services, personal computers, peripherals, or software for personal use;

b) Technology Resource Users will use Multi-Factor Authentication to access City Information when working from a non-corporate Workplace and when working with City Technology Resources where Multi-Factor Authentication is configured; and

c) Technology Resources Users will not connect personal technology devices to The City's network.

3.7 Use of The City's Technology Resources for Personal Purposes

a) City Technology Resources will not be used for any business or commercial activities unrelated to the delivery of municipal services; and

b) Subject to Section 3.5, Technology Resource Users may use City Technology Resources for occasional or incidental personal use that is legal, ethical, and consistent with this and other City policies. Personal use of City Technology Resources that causes a negative impact to The City, such as network

performance, security concerns, abuse of paid work time, or added costs, is not permitted.

4. ROLES AND RESPONSIBILITIES

4.1 All Technology Resource Users are responsible for:

a) Being familiar with and following the behaviors outlined in this policy and its associated standards and procedures;

b) Becoming proficient in the secure use of required City Technology Resources to fulfill work responsibilities as efficiently and effectively as possible;

c) Using City Technology Resources only for their intended purpose or for occasional personal use as outlined in Section 3.7;

d) Using only their own Credentials when using City Technology Resources and keeping their Credentials and Multi-Factor Authentication methods confidential;

e) Using only approved City resources, Multi-Factor Authentication methods, or exceptions approved by the Chief Information Technology Officer to access and store City Information;

f) Not using their Credentials for subscriptions or activities not related to City business;

g) Using only City Credentials for City business purposes and linking to City Technology Resources; and

h) Advising their Exempt Supervisor immediately of any possible violations of this policy.

4.2 Exempt Supervisors are responsible for:

a) Ensuring Technology Resource Users are aware of this policy and its associated standards and procedures;

b) Approving access to City Technology Resources for Technology Resource Users;

c) Approving Technology Resource User requests to purchase City Technology Resources through approved procurement processes;

d) Retrieving and safeguarding City Technology Resources upon the departure of a Technology Resource User;

e) Managing the use of City Technology Resources, including monitoring costs and maintaining asset inventories;

f) Reporting any alleged, suspected, or actual privacy breach to the Access to Information and Corporate Privacy team immediately;

g) Reporting any alleged, suspected, or actual Data breach to the Corporate Security – Cyber Security team immediately; and

h) Reporting any alleged, suspected, or actual breach of this policy to the Chief Information Technology Officer immediately to ensure that City Technology Resources can be safeguarded as quickly as possible.

4.3 The IT Operations and Corporate Security – Cyber Security teams are responsible for:

a) Maintaining cyber security monitoring and detection utilities to filter or restrict content that may pose a risk to The City or violate any City policy;

b) Monitoring, accessing, investigating, auditing, and/or disclosing information related to the use of City Technology Resources, Credentials, and/or City Information to Corporate Security and/or Human Resources for investigative purposes in the event of a suspected breach of this policy; and

c) Removing, deleting, or confiscating any City Technology Resource found to be in violation of this policy or as deemed necessary in emergency situations.

4.4 Information Technology is responsible for:

a) Developing, reviewing, and updating information technology policies, procedures, and guidelines;

b) Governing The City's technology investments;

c) Managing the safety and security of The City's technology environment;

d) Setting standards for City Technology Resources;

e) Providing, managing, and supporting City Technology Resources; and

f) Providing training materials to support the efficient and effect use of Technology Resources.

5. CONSEQUENCES OF NON-COMPLIANCE

5.1 Employees who fail to adhere to this Administration policy or its related 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.

5.2 Contractors who fail to adhere to this Administration policy or its related standards and procedures may be subject to corrective action in accordance with their contracts and agreements.

5.3 Volunteers who fail to adhere to this Administration policy or its related standards and procedures may be subject to appropriate remedial measures including the removal of their access to City Technology Resources and ending their volunteer assignment.

5.4 Any violation deemed criminal in nature will be referred to police.

6. DEFINITIONS

6.1 In this Administration policy:

a) **Artificial Intelligence** means a technology platform that uses statistical algorithms and logic-based technologies such as machine learning and deep learning to simulate human intelligence to perform cognitive functions and solve problems;

b) **Cloud Solution** means a scalable, web-based software application that is provided as a subscription service or storage on the internet through a cloud computing provider;

c) **Credentials** means a Technology Resource User's Electronic Identity, Network Account, or any identity used to access City Technology Resources or access or participate in online services related to City business;

d) **Data** means a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means;

e) **Electronic Identity** means the account login information used to uniquely distinguish each authorized user who has been granted access to City Technology Resources and the Technology Resource User's @calgary.ca email address;

f) **Employee** means any person employed by The City and reporting to a City of Calgary business unit, department, the Office of the Chief Administrative Officer, the Office of the Chief Operating Officer, the Office of The Mayor, the City Auditor's Office, the Calgary Housing Company, and the Calgary Police Service, including those working under an employment contract with The City;

g) **Exempt Supervisor** means any Employee in an exempt position with direct supervisory responsibility for Employees;

h) **Information** means Data in context. It is Data that has been processed, organized, or structured in a way that makes it meaningful to the recipient;

i) **Mobile Device** means a device that uses wireless technology to connect to The City's network, including, but not limited to, tablets, cellular phones, smartphones, air cards, radios, and modems;

j) **Multi-Factor Authentication** means using two or more different methods to validate a Technology Resource User's Credentials before access to a website or application is granted;

k) **Network Account** means authorized login information enabling Technology Resource Users to access applications, shared network drives, and databases connected to The City's network;

l) **Portable Computing Device** means a device that uses wired and/or wireless technology to connect to The City's network, including, but not limited to, notebook computers or laptops;

m) **Removable Device** means any physical media storage device that is used to copy and store information, including, but not limited to, USB sticks (thumb drives), external hard drives, DVDs, and memory cards;

n) **Risk/Value Assessment** means a process conducted by the IT Cloud Computing and Open-Source Program team to help business units evaluate and adopt Cloud Solutions;

o) **Supplier** means a sole proprietorship, partnership, corporation, or other legal entity that offers construction, consulting, goods and services, or information technology for sale, including their employees, representatives, and subcontractors. Supplier may also be referred to as a contractor;

p) **Technology Resources** means any technology that produces, manipulates, stores, communicates, or disseminates information. Examples of Technology Resources include, but are not limited to, computers; mobile computing devices; servers; software; Cloud Solutions and web-based technologies; electronic files; wired and wireless Data; video and voice networks; Internet of Things sensors; modems; augmented reality / virtual reality technology; robots; work-related social media accounts, subscription-based accounts, and registrations; and devices for storing and archiving Information;

q) **Technology Resource User** means any Employee, Volunteer, or Supplier that has been authorized by an Exempt Supervisor to use City Technology Resources;

r) **Volunteer** means an individual who has agreed to perform a service or task at the direction of and on behalf of The City without expecting or receiving compensation; and

s) **Workplace** means a place where an Employee is, or may be, conducting work on behalf of The City, including City worksites, telework locations, online environments, locations travelled to while conducting City-related business, and locations of work-related social gatherings.

7. ASSOCIATED GOVERNANCE

7.1 This Administration policy is established in accordance with the *Municipal Government Act* (Alberta) which describes the responsibility of the Chief Administrative Officer to implement the policies and programs of the municipality.

8. HISTORY

Action	Date	Approval	Description
Clerical Correction	2025 Oct 01	Policy Lead	Administration policy approved on 2025 July 28 transferred to new Administration policy template that came into effect 2025 July 31.
Amendment	2025 July 28	Executive Leadership Team (ELT)	Reviewed and approved by ELT (ELT2025-0765).
Amendment	2016 July 05	Administrative Leadership Team (ALT)	Reviewed and approved by ALT (ALT2016-0391).
Amendment	2012 May 01	Administrative Leadership Team (ALT)	Reviewed and approved by ALT (ALT2012-0378).
Minor Revision	2008 July 01		Migrated to new Administration Policy template. Modified wording of 2.1.1 to include “or its licensors” as requested by the Law department.
New	2003 June 01		New policy.
	1989 Dec 18		Chapter 11: Information Management (In hard-copy-based editions of the Administration Manual).

Proactive Monitoring and Safeguards for Information Systems

The City of Calgary ("The City") protects personal information, data derived from personal information, non-personal data and confidential information ("Information") held across City electronic information systems through a "defense in depth approach": a combination of policies, processes, and safeguards to monitor information systems, identify threats, and prevent unauthorized access. These measures support The City's commitment to protecting privacy while enabling the responsible use of Information to deliver services.

This document describes the alignment of The City's Information protection efforts to the outcomes of the National Institute of Standards and Technology ("NIST") Cyber Security Framework 2.0.

About the NIST Cyber Security Framework 2.0

The NIST framework organizes cyber security activities into six core outcomes. Together, they describe a complete cycle of cyber security risk management.

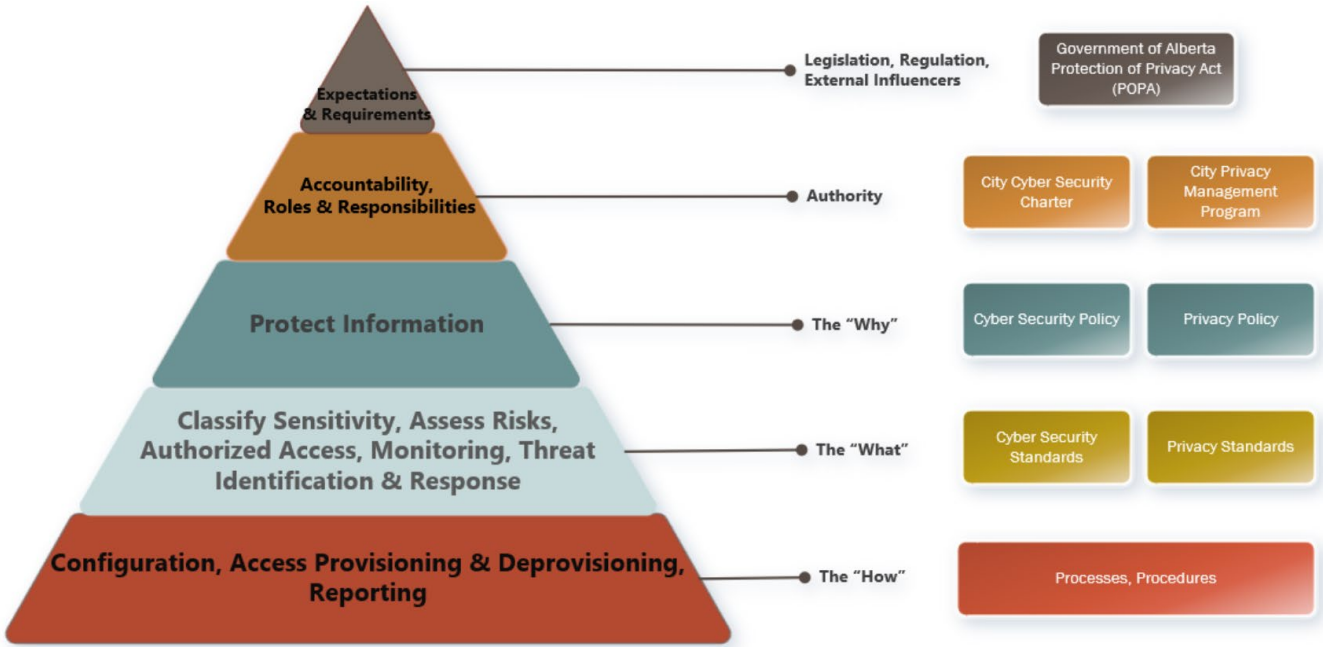
Govern	Identify	Protect	Detect	Respond	Recover
Strategy & Policy	Risk Assessment	Preventive Controls	Monitoring	Incident Response	Restoration

1. Govern – Cyber Security Risk Management Strategy, Policy and Oversight

The Govern outcome establishes and monitors The City's cyber security risk management strategy, expectations, and policies. It provides the organizational context for all cyber security activities.

Policies and Documentation

The City maintains an Administration Policy and Governance Library where cyber security-related policies and standards are published and accessible to employees. A hierarchical structure creates manageable role-based expectations and allows alignment between related functional domains like cyber security and privacy.



Oversight and Accountability

- The City Auditor's Office holds a continuous audit mandate and reviews users' access against authorized users.
- Automated access reviews for cloud environments are monitored through City governance meetings.
- System access requests require documented justification and management approval before access is granted.
- Many business units mandate police background checks as part of their hiring process for City employees who have access to sensitive City systems and information.

2. Identify – Asset Management, Risk Assessment and Supply Chain Risk

The Identify outcome helps The City develop an understanding of its systems, assets, data, and associated cyber security risks, forming the foundation for effective risk management.

Risk Assessments for New or Changed Systems

New technology projects, and any significant changes to existing systems, undergo a cyber security risk assessment before going live. Depending on the system and the Information it holds, this may include one or more of the following:

- Architectural reviews to assess system design and potential risk areas
- Cyber security penetration testing
- Vulnerability assessments
- Web application scanning
- Access control reviews

Systems are also evaluated against The City's Information Security Classification ("ISC") framework to ensure sensitive data, such as personal information and ISC Confidential and Restricted Information, is handled appropriately, and in accordance with its classification.

Vulnerability Management

The City uses automated tools to continuously scan systems to identify known vulnerabilities, allowing us to prioritize patching and updating systems.

Supply Chain Risk Management
When business units procure third-party cloud or software-as-a-service ("SaaS") applications, The City conducts an assessment of the cyber security risks associated with the product, including legal and contract review, before the service is approved for use. Ongoing monitoring responsibilities are defined as part of the procurement process.

Tabletop Exercises
The City conducts regular tabletop exercises to simulate cyber security incidents in a controlled environment. These exercises test The City's response plans, identify gaps in procedures, and build the organizational readiness needed to manage real incidents effectively.

Privacy Compliance and Risk Assessments
A privacy compliance and risk assessment engagement must be completed for any City initiative that involves the collection, use, or disclosure of personal information.

Business Continuity
The City's Business Continuity Planning Policy requires all City business units to maintain up to date business continuity plans, which includes identifying applications used by essential City services and mitigation strategies for various types of disruptions.

Disaster Recovery
The City maintains a Disaster Recovery Plan, focused on recovery of Information assets following a disruptive event.

3. Protect – Safeguards to Prevent or Limit Cyber Security Events

The Protect outcome encompasses the safeguards The City uses to prevent unauthorized access, reduce the attack surface, and maintain accountability for actions taken on City systems.

Administrative Safeguards

- **Automated Access Reviews**
  For most City cloud-based applications, employee access reviews are conducted regularly through automated processes. Supervisors must explicitly confirm whether their direct reports require their current level of access, otherwise access is automatically removed. In some cases, access reviews are performed manually as an ongoing operational maintenance activity by the City division using the service.

- **Cyber Security Awareness Training**
  Employees are required to complete cyber security awareness training on an annual basis. The City also uses simulated phishing attacks to test employees' cyber security awareness.

- **Privacy Awareness Fundamentals Training**
  Employees are required to complete privacy awareness training on an annual basis.

Technical Safeguards

- **User Authentication and Access Controls**
  The City's User Authentication for Enterprise Systems Standard requires defined methods for verifying user identity before access is granted to systems handling personal information, including multi-factor authentication requirements, to reduce the risk of unauthorized access. Multi-factor authentication is also required for remote access to the corporate network. Every user is assigned an individual account, ensuring that actions on City systems can be attributed to a specific person.

- **Change Control**
  Change management processes ensure a standardized approach to maximize efficiency and minimize adverse impacts on IT services and business operations.

- **Firewalls**
  The City uses a layered approach to protect its network and devices, including firewalls to monitor and control traffic.

- **Automated Software Updates**
  Auto-updates are enabled for certain applications across The City's environment, ensuring software remains current and reducing threats.

- **Antivirus Software**
  Corporate antivirus software is deployed across City devices to detect and remove malicious software.

- **Password Controls**
  The City enforces technical controls on passwords across its systems, including requirements for minimum length, complexity, and periodic changes.

- **Encryption**
  Data on portable devices, including phones, tablets, and laptops, is encrypted using full disk encryption or file-based encryption. End user devices, even if not portable, containing sensitive data must use full disk encryption.

- **Email and Web Filtering**
  The City uses email filtering which blocks malicious attachments, suspicious file types and messages based on their content or attributes of the sender. It also uses web-filtering, which stops employees from visiting known malicious or suspicious webpages.

Physical Safeguards

Physical security measures complement The City's digital controls and serve as the foundational layer of protection for Information. Examples include:

- Secured facilities with controlled access to areas where sensitive systems and Information are housed;
- On-site security personnel; and,

- Secure records and Information disposal processes to ensure that physical and digital records containing personal or confidential information are destroyed appropriately.

4. Detect – Timely Discovery of Cyber Security Events

The Detect outcome enables The City to identify cyber security events in a timely manner through continuous monitoring and anomaly detection.

Security Event Monitoring
The City operates a centralized Security Incident and Event Management ("SIEM") system. This platform collects security logs and applies detection rules to identify anomalies or suspicious patterns. Cyber security events are monitored 24/7.

Unstructured Data Monitoring
The City uses dedicated tools to monitor access to files stored on shared network drives. This tooling provides detailed reporting on who is accessing files and when.

Endpoint Threat Detection
The City uses an endpoint threat detection and response tool, which monitors threat indicators, identifies patterns, automatically removes or contains threats, alerts cyber security personnel of incidents, and provides forensic and analysis capabilities. These tools are deployed on workstations, laptops, and servers.

Intrusion Detection Systems
The City employs intrusion detection systems that continuously monitor network traffic for signs of unauthorized access or suspicious activity. These systems generate alerts that are reviewed by cyber security operations staff, enabling timely investigation and response.

Logging and Monitoring User Access
The City requires every user to have their own individual account rather than sharing generic or group accounts. User access to personal information (e.g. viewing, modification, deletion of records) is logged and monitored for various applications in accordance with the Access Control Standard. When possible, The City ensures all locations and systems which contain personal information generate logs which are directed to a security and event monitoring process to identify unauthorized access or suspicious user activity.

5. Respond – Actions Taken in Response to Detected Cyber Security Incidents

The Respond outcome covers The City's ability to take action when a cyber security event is detected — including investigation, communication, and mitigation.

Incident Investigation Capabilities
The City has several capabilities that support effective response when a cyber security incident occurs:

- The centralized SIEM system enables cyber security operations staff to correlate alerts across systems, accelerating investigation and scoping of incidents.
    - Logging across City systems provides activity records to support forensic review when an incident occurs.
    - Individual user account requirements mean that suspicious activity can be attributed to a specific person, reducing investigation time, and improving accountability.

- A structured, approval-based process governs access to sensitive content for the purposes of investigation, with documented rationale and management approval required before access is granted.

Physical Corroboration
Physical security measures have been used to support investigations in situations where digital audit trails were incomplete. This multi-layered approach ensures The City can investigate incidents even when technical records alone are insufficient.

6. Recover – Restoring Capabilities Affected by Cyber Security Incidents

The Recover outcome supports The City's ability to restore normal operations and services following a cyber security incident, and to improve based on lessons learned.

Automated Backups and Data Restoration
The City requires frequent automated backups of City data, with backup frequency and standards defined based on the criticality of the Information. These backups enable The City to restore data to a prior state in the event of accidental deletion or corruption..

Continuous Improvement
The City conducts a post-incident reviews to identify lessons learned and opportunities to strengthen its controls. Findings from these reviews, as well as from tabletop exercises and third-party assessments, are used to update policies, improve technical safeguards, and enhance staff training. This commitment to continuous improvement ensures that The City's cyber security posture evolves alongside the threat landscape.

Administration Standard

Title:	**Information Security Classification**
Effective Date:	**2026 June 04**
Responsible Business Unit:	**Cyber Security**

GENERAL

This Standard is an extension of the Information Management and Security Policy. Consequences of non-compliance with this Standard are outlined in the Policy.

PURPOSE

The City's *Information Security Classification Standard* specifies classification and protection measures that must be consistently applied to The City's Information Assets.

In addition to supporting The City's information security requirements, appropriate information classification supports The City's objectives of transparency, accessibility of information both internally and to the public, and by helping to identify Information Assets that can be made available for routine disclosure to the public or as part of Open Data initiatives.

SCOPE

This Administration standard applies to City of Calgary employees.

Calgary Police Service employees are exempt, except when they use City of Calgary accounts to access City services.

This Administration standard also applies to Volunteers and Suppliers.

DEFINITIONS

"Authorized User" means an individual who has been granted access to use City Information Assets or Information Systems; Authorized Users may be internal users (City employees) or external users;

"Availability" means the accessibility of Information and Information Systems to ensure minimal disruption of service;

"City-Managed" means Information Systems owned and operated by The City of Calgary or those operated by others in an approved contractual relationship with The City, whether on City premises or off-premises (i.e. cloud services);

"**Confidential**" means the information so classified is valuable or sensitive to The City or requires protection by law, regulation, agreement, or City policy;

"Confidentiality" means the state of keeping or being kept private; ensuring Information, documents, Data, etc. are limited to authorized persons only;

"Data" means any facts, concepts, quantities, characters, or instructions stored and/or transmitted in electronic formats;

"Data Derived From Personal Information" means data (i) created by data matching, and (ii) that identifies any individual whose personal information was used in the data matching;

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

"Information" means any collection of Data that is processed, analyzed, interpreted, classified, or communicated to serve a useful purpose, present facts, or represent knowledge;

"Information Asset" means information recognized as having value for the purpose of enabling The City to perform its business functions, thereby satisfying a recognized business requirement. There are many types of Information Assets. Information Assets can include Data and Intellectual Property. May be used interchangeably with "Information" in this standard.

"Information Steward" means any Authorized User given responsibility for the management of specific Information Assets or Information Systems.

"Information System" means any set of components used to handle Information. Information Systems include applications, services, or any other assets that handle Information;

"Integrity" means assurance of the accuracy and reliability of the Information and Information Systems is provided and any unauthorized modification is prevented.

"Intellectual Property" means all trademarks, copyrights, art, inventions, creative works, reports, Data, compilations of information, computer programs, drawings, sketches, layouts, commercial material, working papers, documents, copy, ideas, photographs and negatives, films, videotapes, video, audio and audio-visual productions and other materials in all forms and however fixed, stored, expressed, or embodied, created, developed, generated, authored, or produced;

"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 *Protection of Privacy Act* ministerial regulations;

"Personal Information" means the recorded information about an identifiable individual as defined in Section 1(q) of the Alberta *Protection of Privacy Act ("POPA")*

"Privacy Risk Questionnaire" (**PRQ**) means the intake form used to initiate privacy compliance and risk assessment to determine whether a City initiative requires a Privacy Impact Assessment;

"Privacy Impact Assessment" (**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;

"**Restricted**" means the information so classified is of high value or sensitivity to The City and, if compromised, could put The City at financial or legal risk. Restricted classification of certain information may also be required by law, regulation, agreement, or City policy.

"Service Owner" means an individual responsible for representing the service on behalf of the Administration.

"**Unrestricted**" means the information so classified is unlikely to cause harm to individuals or to The City if released publicly. This is the default classification.

STANDARD DETAILS – CLAUSES AND SUBCLAUSES

ROLES AND RESPONSIBILITIES

Users

All Authorized Users of Information and Information Systems must:

- Classify Information they create in accordance with the requirements of this Standard
- Label all Information they create according to the three classification levels defined in this Standard
- Recognize the classification ratings assigned to Information Assets created by others and safeguard those assets accordingly
- Complete Information Security Classification training

Information Stewards

Information Stewards must:

- Manage specific Information Assets or Information Systems including ensuring that information they are responsible for is classified properly
- Take steps to secure Information Assets or Information Systems according to their classification level
- In the event of a classification change, ensure that Cyber Security is engaged for an analysis of security controls to determine whether existing security controls are consistent with the new classification
- If gaps are found in existing security controls, work with relevant groups (Information Technology, Cyber Security, Information and Privacy Services, etc.) to address the resulting risk(s)

Service Owners

Service Owners must:

- Designate themselves or another Authorized User as the Information Steward for each service they are accountable for
- Identify the security classification level of all service-related information and Information Systems
- Reevaluate the classification of Information Assets as required by a change in the type of Information, change in business process or change in technology to ensure the assigned classification is still appropriate
- Maintain awareness of the security classification level and the effectiveness of implemented security controls, even if not acting as an Information Steward.

Managers and Supervisors

Managers and Supervisors must:

- Ensure that all their direct reports are made aware of this Standard and its corresponding guidelines
- Ensure that all direct reports understand the importance of classifying, labelling, and safeguarding Information
- Complete the Information Security Classification training and oversee its completion by all direct reports

Cyber Security

Cyber Security must:

- Maintain this Standard and the corresponding guidelines
- Provide Standard interpretation and guidance as required
- Provide tools to raise awareness about the requirements in this Standard and help all users meet their obligations to implement them
- Provide cyber security services as may be required to assist Business Units in the implementation of this Standard

Information Technology

Information Technology must:

- Provide, or assist with, electronic Information and document management practices as appropriate
- Work with Cyber Security to ensure that appropriate security tools and services are made available to enable the appropriate safeguarding of Information and Information Systems of all classification levels
- Provide hosting and storage environments that enable the appropriate safeguarding of Information and Information Systems of all classification levels
- Ensure that Information Assets enter and exit The City in compliance with the Access and Sharing Standard
- Collaborate with internal Authorized Users to ensure that Data is made available through the proper self-service portal (e.g., Open Data or City Online)

Information and Privacy Services

Information and Privacy Services must:

- Work with Cyber Security and Information Technology to ensure legislative requirements under the *Protection of Privacy Act ("POPA")* and the *Municipal Government Act* are addressed in this Standard and related standards, procedures, and guidelines.
- Coordinate the Corporate Records Management Program activities throughout The City, including retention and disposal of Information.

INFORMATION SECURITY CLASSIFICATION

The City uses the following three information security classifications:

Classification	Unrestricted	Confidential	Restricted
Definition	Information that is unlikely to cause harm to individuals or to The City if released publicly This is the default classification.	Information that is valuable or sensitive to The City or requires protection by law, regulation, agreement, or City policy. This includes personal information, data derived from personal information and non-personal data.	• Information that is of high value or sensitivity, that if compromised, could put The City at financial or legal risk. • Information that is required to be treated as Restricted by law, regulation, agreement, or City policy.
Risks of Unauthorized Distribution, Modification or Loss	• Little or no impact to reputation • Minimal inconvenience if not available • Minimal financial loss	• Loss of reputation or competitive advantage • Loss of confidence in a City program • Reduce the level of public trust in The City • Penalties for violating the *Protection of Privacy Act* • Loss of trade secrets or Intellectual Property • Loss of potential revenue • Damage to partnerships • Reputational harm to an individual	• Significant loss of reputation or competitive advantage • Serious loss of confidence in a City program • Substantial reduction of the level of public trust in The City • Injury or loss of life • Extreme impact to public safety • Catastrophic financial loss • Catastrophic damage • Sabotage and terrorism

	Unrestricted	Confidential	Restricted
Examples	• Most internal correspondence • Published Council Meeting Minutes & Agendas • White papers • Most meeting minutes • Fee schedules • Building permit files • Public Health and Safety information • Job titles, job descriptions, pay scales • Information received from partners or government that is freely available in the public domain	• Employee usernames, employee identification numbers and passwords • Personal or financial Information related to individual citizens or businesses • Highly valued Intellectual Property • Material prepared for in-camera Council meetings • Material subject to legal privilege • Testing and auditing procedures • Negotiation Information related to suppliers and third parties • Contracts	• Architectural plans for sensitive facilities and critical infrastructure • Security procedures • Items of high political or legal sensitivity • Information which The City is required to classify and protect as Restricted by law, contract, or agreement • Where the potential loss from unauthorized disclosure, alteration or unavailability of Information is expensive
Multi-class Information	If the Information System or Information Asset contains sections with different information security classifications, reasonable efforts must be made to separate out and/or make available the Unrestricted portions. If the sections cannot be separated, then the highest level of classification and protection must be applied to ALL the Information.		

If there is any ambiguity between two levels with respect to classification, the Information must be classified at the higher level until it can be definitively classified.

INFORMATION ASSET PROTECTION REQUIREMENTS

Information Assets must be protected in accordance with their information security classification.

The minimum protection requirements necessary at each security classification level are specified in appendices to this Standard.

- Appendix A: Storing City Information
- Appendix B: Communication of City Information
- Appendix C: Labelling of City Information
- Appendix D: Disposal of City Information

The appendices will be updated as required due to technology changes, availability of new controls, and changes to the threat landscape.

Information assets must be managed throughout their lifecycle (creation, use and disposal), according to the Records Management Administration Policy and the Corporate Records Management Program.

Appendix A: Storing City Information

	Unrestricted	Confidential	Restricted
Hard Copy Information			
	No security-specific storage requirements	Must be locked in an office, desk or filing cabinet when unattended	Must always be attended or physically secured e.g. Locked in a secure filing cabinet or secure room
Electronic Information – Original and Authoritative Versions			
	Original and authoritative versions of all City information must be stored on City-managed storage.		
Network Drives (available on the corporate network, e.g. H:, S: drives)	Allowed	Allowed with appropriate access restrictions in place. Encryption recommended.*	Allowed with appropriate access restrictions in place. Encryption required.*
Content Server	Allowed	Allowed with appropriate access restrictions in place. Encryption recommended.*	Allowed with appropriate access restrictions in place. Encryption required.*
City-managed Cloud Services (e.g. OneDrive)	Allowed	Allowed. Information is encrypted by default.	Not Allowed
City-managed Cloud-based Collaboration Platforms (e.g. Microsoft Teams)	Allowed	Allowed. Information is encrypted by default.	Not Allowed
Other Cloud Services	Third party services may only be used when approved by Corporate Cloud Computing Stakeholders Team		Not Allowed
* Consult with Cyber Security and IT.			

	Unrestricted	Confidential	Restricted
Electronic Information – Temporary Copies			
	• Temporary copies of City Information for sharing or for offline use following an approved business process may be stored only as described below. • If the business process requires that changes to a temporary copy be reflected in the original version, appropriate measures must be taken when copying or synchronizing with the original Information to ensure the Integrity of the Information is maintained.		
Storage of a copy on City-managed Device (e.g. C: drive of a laptop or PC, iPhones, iPads)	Allowed	Allowed Information is encrypted by default.	Not allowed
Storage of a copy on removable media (e.g. USB stick, CD, DVD, external disk drive)	Allowed	Not allowed	Not allowed

Electronic Information – Non-Employees	
	Contractors, consultants, and other non-employees must use only City-managed devices, platforms, or cloud services to process or store City Information unless this is explicitly permitted by the terms of their contract or approved in writing by their City contract manager. The Information concerned must be appropriate to the provisions of that contract.

	Unrestricted	Confidential	Restricted
Electronic Information – Access Control and Audit Logs			
Access Controls	No special procedures. May be required for business purposes.	• Use of role-based access controls required • Access via City network or VPN	• Use of role-based access controls required • Access via City network or VPN
Audit Logs	No special procedures. May be required for business purposes.	• Logging must be enabled and active for all systems • Audit logs must be promptly backed up and automatically analyzed • Anomalies identified must be reviewed by Cyber Security	

Care must be taken to protect the Integrity and Availability of Unrestricted Information published electronically to prevent unauthorized modification that could harm the reputation of The City.

For any cases not covered above, consult with Cyber Security.

Appendix B: Communication of City Information

	Unrestricted	Confidential	Restricted
Internal Sharing	Internal sharing of Information Assets is encouraged wherever possible and appropriate to further business activity and facilitate knowledge reuse. Send requests to the appropriate Information Steward. Internal disclosure of Personal Information and Data Derived from Personal Information should be consistent with the purpose of its collection or creation and **may require a Privacy Risk Questionnaire or a Privacy Impact Assessment.**		May only be shared on a strict need-to-know basis and only with a minimum number of explicitly named individuals.
External Sharing	Allowed	Personal Information: • Disclose only in accordance with Section 13 of the *Protection of Privacy Act*, or as authorized by applicable law. Non-personal data: • Allowed to disclose to any public body for any purpose. • Disclosure to other than a public body requires a signed agreement. May require a Privacy Risk Questionnaire or a Privacy Impact Assessment.	Not allowed
	The above is general guidance only. Refer to the ***Access and Sharing Standard*** and consult with Law and the Access to Information and Corporate Privacy team for advice on internal and external sharing of City of Calgary Information Assets.		

	Unrestricted	Confidential	Restricted
Hard Copy Information			
Transfer (Mail, Courier, Internal Mail)	No special procedures	• Sealed confidential envelope • Use only a reputable company or a trusted employee.	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) • Handled under a continuous chain of custody with receipts documenting everyone who obtained custody • Use only a reputable company or a trusted employee. • Only the inner envelope is to be labelled with "Restricted" • Consider enclosing an acknowledgement slip to be signed by the recipient, confirming understanding of Restricted precautions.
Electronic Information			
Transmission (e.g. SMTP (Email), SFTP, HTTPS)	No special procedures	• City-approved encryption must be used • Confidential Information contained in or attached to email must be encrypted • Consider including handling instructions for the recipient, including disposal instructions.	• Must never be transmitted in unencrypted form • Consult with Cyber Security prior to implementing encrypted transmission of Restricted Information • Include handling instructions for the recipient, including disposal instructions.

<table>
<tr><th></th><th>Unrestricted</th><th>Confidential</th><th>Restricted</th></tr>
<tr><td>Public conversations</td><td>Be cautious to limit discussion of City of Calgary business in public locations.</td><td colspan="2">Take care so that only those with a need to know can hear your conversation. Special care should be taken in discussing sensitive Information when traveling to or participating in meetings away from City of Calgary work sites.

Confidential or Restricted Information should be clearly identified as such to all participants in the conversation.</td></tr>
<tr><td rowspan="2">Photocopying & Printing</td><td rowspan="2">No special procedures</td><td>Carried out or supervised by the originator, a trusted nominee, or a trusted service organization that has signed a non-disclosure agreement.</td><td>Carried out or supervised by the originator, a trusted nominee, or a trusted service organization that has signed a non-disclosure agreement. Each copy must be tracked and marked with a unique number. (e.g. 1 of 10, 2 of 10, etc.)</td></tr>
<tr><td colspan="2">Be aware that printers and photocopiers usually retain a copy of the document on internal storage (i.e. hard disk) until the space is required for other documents. (Possibly weeks or months, depending on usage.)</td></tr>
<tr><td>Faxes, receiving</td><td>No special procedures</td><td colspan="2">Consult with IT and Cyber Security.</td></tr>
<tr><td>Faxes, sending</td><td>Check that the correct fax number is dialed and that the cover sheet is correctly completed.</td><td>Because most fax machines can store messages, physical access to both the sending and receiving machine should be limited to authorized individuals.</td><td>Faxing Restricted Information is very strongly discouraged. Because most fax machines can store messages, physical access must be limited to authorized individuals.
Prior arrangements must be made with the recipient to ensure that the receiving machine is attended by a trusted nominee or secured in a locked cabinet or room.</td></tr>
</table>

	Unrestricted	Confidential	Restricted
City of Calgary internal telephone	Allowed	Allowed Consider the possibility of being overheard.	Safe for City office-to-office Restricted communication. Consider the possibility of being overheard.
Normal wired telephone lines (non-City of Calgary)	Allowed	Use caution and bear in mind that telephone lines may be intercepted. Avoid unnecessary mention of sensitive items.	Should not be used for Restricted communication. If use is unavoidable, use pre-arranged code words to avoid references to individuals, companies, and projects.
Voice Calls on City-managed cell phones & smartphones	Allowed	Avoid unnecessary mention of confidential items	Use for Restricted communication is very strongly discouraged. If use of cell phone is unavoidable then consider using pre-arranged code words for individuals, companies, projects, etc.
Text Messages on City-managed cell phones & smartphones	Allowed	Text messages can be intercepted. Sending numbers can be impersonated. Avoid unnecessary mention of confidential items	Use for Restricted communication is very strongly discouraged. If use of text messaging is unavoidable then consider using pre-arranged code words for individuals, companies, projects, etc.

	Unrestricted	Confidential	Restricted
Voicemail (City Internal and City Cellular)	Allowed	Confidential Information should be left only with caution. Consider extra precautions, e.g. an introductory message not to listen via speakerphone and a suggestion to delete the message.	Restricted Information must not be left in a voice mail message
Voicemail (Personal, Other Organizations)	Allowed	Not Allowed	Not Allowed
City-Managed Teleconference & Videoconference Systems (i.e. Microsoft Teams)	Allowed	Allowed	Consult with IT and Cyber Security.
Non-City-Managed Teleconference & Videoconference Systems (e.g. Zoom, WebEx, apps with video calling)	Allowed	Not Recommended If used, be confident of the identities of the participants before disclosing Confidential Information. Be aware that recordings can occur without notice to participants.	Not Allowed
Hotel telephones	Allowed	Not recommended. Hotel phones, including lobby/courtesy phones, are insecure.	Not Allowed
Public telephones	Allowed	Not recommended. May be easily overheard and operated with minimal security.	Not Allowed

	Unrestricted	Confidential	Restricted
Non-City-Managed Internet Voice Services **(e.g. Google Voice, WhatsApp, Snapchat, Messenger)**	Allowed	Not allowed	Not allowed
Outlook Calendar	Allowed	Confidential meeting details or attachments available through Outlook Calendar must be hidden from view by flagging the meeting as “Private”.	Do not include Restricted Information in the body or attachments to a calendar item. A link to an access-controlled location may be included.
		Caution: When a user’s calendar is shared, meeting agendas and distributed attachments are also viewable by those with access to the shared calendar.	
Internal meetings and conferences	Allowed	Hold meetings behind closed doors.	Hold meetings behind closed doors. Consider maintaining a secure room (kept locked when not in use) for regular meetings.
Presentations **(e.g. PowerPoint, flipcharts, printed media)**	Allowed	• Information displayed must not be viewable by unauthorized persons (e.g. open doors or outside windows). • All items should be clearly marked ‘ISC: Confidential’; this should also be displayed when projected for viewing • Ensure all Confidential Information is collected or destroyed afterwards.	• Information displayed must not be viewable by unauthorized persons (e.g. open doors or outside windows). • All items must be clearly marked ‘ISC: Restricted’; this should also be displayed when projected for viewing • Ensure all documents are collected or destroyed afterwards. • Remind participants of how to treat Restricted Information.

	Unrestricted	Confidential	Restricted
External meetings and conferences	Allowed	Do not disclose meeting to non-attendees.	Do not disclose meeting to non-attendees.
		Hold meetings behind closed doors. Discretion should be used in choosing a suitable location.	Hold meetings behind closed doors. Use caution in selecting a location. Advice should be sought from City of Calgary Corporate Security. Consider carrying out a search for eavesdropping devices.
		See Presentations: Ensure all Confidential information is collected or destroyed afterwards.	See Presentations: Ensure all Restricted information is collected or destroyed afterwards.

Appendix C: Labelling of City Information

	Unrestricted	Confidential	Restricted
Hard Copy Information			
Hard Copy Information	No special procedures. If unlabeled, the document is considered Unrestricted by default.	Include "ISC: Confidential" clearly on: • each page of the document. • file folder labels • boxes containing Confidential Information	Include "ISC: Restricted" clearly on: • each page of the document. • file folder labels • boxes containing Restricted Information. Serially number each copy (e.g. No. 2 of 8 copies). • Assign each copy number to a named individual.
Electronic Information			
Email	No special procedures. If unlabeled, the email is considered Unrestricted by default.	Include "Confidential" in the subject line of email to inform the recipient of its classification.	Include "Restricted" in the subject line of email to inform the recipient of its classification. Refer to Restricted email conditions in Appendix B.
Files/folder names	No requirements.	Electronic documents (files), folders and directories should not have “Confidential” within their names.	Electronic documents (files), folder and directories should not have “Restricted” within their names.
Databases and Business Applications	Identify classification of data in system/application metadata. All applications and databases housing Confidential or Restricted information must be secured and have appropriate protection.		
Other Electronic Information and Documents	Identify the classification in the document’s metadata. If additional classification options are available as part of a document management system, they must be used.		
		Where possible, include "ISC: Confidential" clearly on each page of the document.	Where possible: • Include "ISC: Restricted" clearly on each page of the document. • Serially number each copy (e.g. No. 2 of 8 copies). • Assign each copy number to a named individual.

Appendix D: Disposal of City Information

For all Information, including Corporate Records, the following disposal methods must be used.

	Unrestricted	Confidential	Restricted
Hard Copy Information			
Paper documents	Throw out or recycle. Shredding should be considered for documents containing valuable or sensitive information even if it does not meet the criteria for a Confidential classification.	Crosscut shred, or place in a locked container that has been designated for Confidential document collection and disposal.	Crosscut shred, or place in a locked container that has been designated for Restricted document collection and disposal. Log disposal details.
	Contact Corporate Security for guidance on required shredder specifications.		
Electronic Information			
City-Managed Storage	Delete and empty the Recycle Bin (or equivalent depending on the device or system)	Same as Unrestricted. Confidential Information must be stored in an encrypted format, so it will be unreadable even if recovered.	Contact IT and Cyber Security for assistance
Cloud Services	Certificate of Destruction from cloud service provider is recommended.	Certificate of Destruction from cloud service provider is required.	
Devices containing electronic files **(e.g. City of Calgary PCs, Laptops, Servers, Phones, Tablets, Disk Drives, Removable Media)**	City of Calgary IT's processes must be used to ensure secure deletion of information and disposal of the device, if required. If returning a device to IT: • If possible, delete Confidential or Restricted files • Inform IT if the device contained or still contains Confidential or Restricted Information If redeploying within your business unit: • Contact IT for assistance in securely erasing any information on the device • Do not redeploy the device before it is securely erased. Reformatting the device's storage is not sufficient.		

RESOURCES

Refer to the Administration Policy Library for the following:

Information Management and Security Policy

Corporate Records Management Policies and Program

Protection of Privacy Policy

HISTORY

Action	Date	Approval	Description
Minor Revision	2026 Jun 04	Director, Corporate Security	Updated multiple sections to align with new legislation and updates to the Protection of Privacy policy and its supporting standards.
Clerical Correction	2026 Jan 19	Leader, Governance and Policy	Changed Title Block to refer to Responsible Business Unit instead of Responsible Service.
Minor Revision	2022 Dec 13		Revised descriptions of Information Security Classification levels; expanded and reorganized Information Asset Protection Requirements; added definitions and roles & responsibilities
New	2018 Jan 30	Information Management and Security Governance Committee	New Information Security Classification Standard reviewed and approved by Information Management and Security Governance Committee.

Administration Standard

Title:	**Privacy Compliance and Risk Assessment**
Effective Date:	**2026 June 01**
Responsible Business Unit:	**Law, Legislative Services & Security – Information & Privacy Services**

1. PURPOSE

1.1 This standard will be followed when:

a) The City collects, uses, discloses or destroys personal information in its custody or under its control;

b) The City creates and discloses data derived from personal information and non-personal data; and,

c) The City has a new or substantial changes to an existing administrative practice, program, project, or service (collectively "City initiative") involving personal information, data derived from personal information and non-personal data.

1.2 Following this standard will result in:

a) Strengthening privacy and transparency by clearly identifying how personal information, data derived from personal information and non-personal data are managed;

b) Complying with The City's obligations under the *Protection of Privacy Act* ("*POPA*") and *POPA (Ministerial) Regulations* ("*Ministerial Regulation*"); and,

c) Demonstrating that privacy was considered, reasonable steps were taken to identify risks, and recommendations to mitigate the identified risks were provided.

2. APPLICABILITY

2.1 This Administration standard applies to all City employees except:

a) Elected officials;

b) Calgary Housing Corporation employees; and,

c) Calgary Police Service employees.

3. STANDARD

3.1 When employees are involved with a City initiative that includes the collection, use, or disclosure of personal information, they must fulfill the following responsibilities:

a) Initiate privacy compliance and risk assessment engagement with the Privacy Officer;

b) Work with their business unit Access and Privacy Program Administrator (“APPA”) to ensure that all relevant information with respect to all City initiatives that involve the handling and management of personal information, data derived from personal information and non-personal data is submitted to the Privacy Officer;

c) Participate in the privacy compliance and risk assessment engagement and collaborate with the Privacy Officer to identify and address potential privacy risks associated with:

i. Collection, use and disclosure of personal information;

ii. Creation of data derived from personal information and non-personal data;

iii. Storage, security, accuracy, retention and destruction of personal information, data derived from personal information and non-personal data; and,

iv. Personal information flows.

3.2 Access and Privacy Program Administrators (“APPA”) will:

a) Assist their business unit to complete the Privacy Risk Questionnaire (“PRQ”) and/or Privacy Impact Assessment (“PIA”) intake forms to initiate the engagement with the Privacy Officer;

b) Maintain a business unit inventory of PRQ and PIA outcomes;

c) Support their business unit in implementing privacy protection measures;

d) Evaluate new City initiatives or substantial changes to programs, involving personal information, data derived from personal information and non-personal data, and consult with the Privacy Officer; and,

e) Assist the Privacy Officer with the follow-up process for the implementation of recommendations from the PIA report.

3.3 Business Unit Managers will:

a) Ensure implementation of privacy risk mitigation recommendations identified in the PIA report, or ensure that an alternate mitigation strategy is developed and implemented; and,

b) Be accountable for the privacy risks associated with their City initiatives, and taking steps to mitigate the risks.

3.4 Project Team or Business Process Owner is responsible for:

a) Identifying a submitter to initiate the PRQ and act as a conduit in communicating the results, associated privacy recommendations and follow-up requests;

b) Participating in the completion of the PRQ and/or PIA in consultation with other affected business unit(s) including fact-checking the information about the initiative and providing associated project documentation;

c) Alerting the APPA and Privacy Officer if changes are made to a City initiative or service involving personal information;

d) Implementing privacy recommendations from the PIA report in a timely manner, as deemed appropriate, or implementing an alternative mitigation strategy; and,

e) Conducting an annual review of each PIA for multi-year initiatives to ensure information in the PIA reflects current practices.

3.5 The Privacy Officer will:

a) Develop, implement and manage the privacy compliance and risk assessment process at The City;

b) Receive and validate PRQ and PIA submissions, including consulting with the project team or submitter and returning incomplete submissions and providing privacy guidance;

c) Determine if a City initiative requires a PIA to be conducted by conducting a PRQ assessment;

d) Conduct, in collaboration with the business unit, PIAs as prescribed by and in compliance with *POPA* and *Ministerial Regulation* by documenting reasonable security arrangements in place, privacy risks and mitigation strategies respecting personal information, data derived from personal information and non-personal data;

e) Issue written PIA reports based on the privacy risk assessment findings, with recommended privacy risk mitigations;

f) Comply with the mandatory submission of PIA reports to the Office of Information and Privacy Commissioner ("OIPC") of Alberta, as prescribed in *POPA* and the *Ministerial Regulation*;

g) Publish summaries of completed PIAs on The City's website; and,

h) Conduct a follow-up with Business Unit Managers within six months after issuing a PIA report, to determine if they have considered the PIA recommendations or if they need assistance in implementing the recommendations or alternatives.

4. CONSEQUENCES OF NON-COMPLIANCE

4.1 Employees who fail to adhere to this Administration standard 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.

4.2 In addition to any consequences from The City associated with not adhering to this Administration standard, failure to comply with the duties imposed by the *Protection of Privacy Act* or otherwise acting in contravention of the legislation may be an offence under the *Protection of Privacy Act*, which could result in penalties.

5. DEFINITIONS

5.1 In this Administration standard:

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

b) **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;

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

d) **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*;

e) **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*;

f) **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.

g) **Privacy Officer** means the person designated or identified to ensure The City's compliance with *POPA*.

h) **Privacy Compliance and Risk Assessment** engagement includes the Privacy Risk Questionnaire and the Privacy Impact Assessment.

i) **Privacy Risk Questionnaire** or **PRQ** is an intake form used to initiate privacy compliance and risk assessment to determine whether a City initiative requires a PIA;

j) **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; and

k) **Project Team or Business Process Owner** means individuals who are familiar with The City initiative associated with the privacy compliance and risk assessment.

6. ASSOCIATED GOVERNANCE

6.1 This administration standard outlines requirements in support of the *Protection of Privacy policy*.

6.2 This administration standard conforms to *Protection of Privacy Act* ("*POPA*") and *Protection of Privacy (Ministerial) Regulation* ("*Ministerial Regulation*").

6.3 If any provision of this administration standard conflicts with any provision of *POPA* or *Ministerial Regulation,* the enactment prevails.

7. HISTORY

Action	Date	Approval	Description
New	2026 Jun 01	Head of the Local Public Body	New Standard developed during the review of the Protection of Privacy policy. Replaces the former Privacy Impact Assessment Standard, which was rescinded effective 2026 June 01.

Administration Standard

Title:	**Consent to Use or Disclose Personal Information**
Effective Date:	**2026 June 01**
Responsible Business Unit:	**Law, Legislative Services & Security – Information & Privacy Services**

1. PURPOSE

1.1 This Administration standard will be followed by The City of Calgary ("The City") when obtaining an individual's consent to use or disclose their personal information.

1.2 The rules for how The City is authorized to use and disclose the personal information in its custody or under its control are set out in the *Protection of Privacy Act* ("*POPA*"), *Protection of Privacy Regulation*, the *Protection of Privacy (Ministerial) Regulation* and other applicable law (collectively, "applicable law").

1.3 Where the use or disclosure of an individual's personal information is not otherwise authorized by applicable law, that individual may provide consent for The City to use or disclose their personal information.

1.4 Consent of a minor, under age 18, is not valid unless The City has determined, on reasonable grounds, that the minor has the capacity to understand the information relevant to providing consent and appreciates the consequences of providing consent.

1.5 Consent obtained under this Administration standard may be provided orally, electronically or in writing.

1.6 Following this Administration standard will result in:

a) Consent practices that are compliant with applicable law; and

b) Increased public trust through consistent and transparent practices, ensuring individuals understand how consent may be provided for The City to use or disclose an individual's personal information.

2. APPLICABILITY

2.1 This Administration standard applies to all City employees except:

a) Elected officials;

b) Calgary Housing Corporation employees; and,

c) Calgary Police Service employees.

3. STANDARD

3.1 Employees will:

a) Require consent when required by applicable law, policy or as informed by legal advice prior to using or disclosing personal information when not otherwise authorized by applicable law;

b) Ensure that consent obtained in any form is informed and voluntary;

c) Ensure that consent specifies:

   i. The personal information to which the consent relates;

   ii. To whom the personal information may be disclosed and how the personal information may be used; and

   iii. The date on which the consent is effective, and, if applicable, the date on which the consent expires.

d) Advise the individual that their consent, once given, may be withdrawn at any time, and provide contact information for withdrawing consent;

e) If consent is withdrawn, ensure that the use or disclosure of the personal information ceases immediately upon receipt of the withdrawal;

f) Ensure that the form of consent accepted by The City (oral, electronic or written) is explicitly communicated to the individual;

g) Authenticate the identity of the individual in accordance with policies and procedures established by the business unit;

h) Accept written consent as valid if it is physically signed by the individual;

i) Accept oral, electronic or written consent only when the individual provides all information specified in subsections 3.1(b) and 3.1(c);

j) Retain the electronic or written consent so that it is accessible by The City and useable for subsequent reference, in accordance with The City's Corporate Records and Classification Retention Schedule ("CRCRS").

k) Retain a recording of the oral consent so that it is accessible by The City and useable for subsequent reference, in accordance with The City's CRCRS.

3.2 Business Unit Managers will:

a) Identify all business unit activities that require consent to use or disclose an individual's personal information;

   i. For each business unit activity, establish a process for:

      a. obtaining consent, including whether consent is to be obtained orally, electronically or in writing, ensuring the process is appropriate and proportionate to the sensitivity and identified level of risk of the personal information involved;

      b. authenticating the identity of the individual which may include, valid:

         - Government-issued photo identification;
         - City account or secure login credential; or
         - A previously established identity verification process, such as DocuSign.

b) Document all established processes for obtaining consent to use or disclose an individual's personal information.

4. CONSEQUENCES OF NON-COMPLIANCE

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

4.2 In addition to any consequences from The City associated with not adhering to this Administration standard, failure to comply with the duties imposed by the Acts or otherwise acting in contravention of the legislation may lead to penalties or offences under *POPA*.

5. DEFINITIONS

5.1 In this Administration standard:

a) **Business unit** means the City business unit obtaining oral, electronic or written consent from the individual providing consent;

b) **Electronic** includes created, recorded, transmitted or stored in digital form or in any other intangible form by electronic, magnetic or optical means or by any other means that have similar capabilities for creation, recording, transmission or storage;

c) **Electronic consent** means a consent executed by the individual using an electronic signature that can be linked or attached to an electronic record;

d) **Electronic signature** means electronic information that a person creates or adopts in order to sign a record and that is in, attached to or associated with the record, including a digital signature created through a platform such as DocuSign or typing a name in a box that indicates that they are signing;

e) **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*;

f) **Individual** means the individual providing oral, electronic or written consent for The City to use or disclose that individual's personal information;

g) **Informed consent** means meaningful consent in which individuals understand the nature, purpose and consequences of what they are consenting to;

h) **Personal information** means recorded information about an identifiable individual;

i) **Record** means a record of 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; and

j) **Record of oral consent** means an audio recording of the consent created by or on behalf of The City.

ASSOCIATED GOVERNANCE

5.1 This Administration standard outlines requirements in support of the *Protection of Privacy policy*.

5.2 This Administration standard conforms to applicable law.

5.3 If any provision of this Administration standard conflicts with any provision of applicable law, the provision of the applicable law prevails.

6. HISTORY

Action	Date	Approval	Description
New	2026 Jun 01	Head of the Local Public Body	New Standard developed during the review of the Protection of Privacy policy.