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. |