Category: Administration Standard

Title:	**Privacy Impact Assessment (PIA)**
Adopted by:	**Director/City Clerk**
Effective Date:	**March 22, 2024**
Last Updated:	**March 22, 2024**
Responsible Service(s)	**Records Management, Access and Privacy**

1. ASSOCIATED GOVERNANCE

1.1. This administration standard outlines requirements in support of the Protection of Privacy Administration Policy.

1.2. This administration standard conforms to the *Freedom of Information and Protection of Privacy ("*FOIP Act*")* RSA 2000, Chapter F-25, as amended.

1.3. If any provision of this administration standard conflicts with any provision of the FOIP Act, the provision of the FOIP Act prevails.

2. PURPOSE

2.1. This administration standard shall be followed to ensure The City of Calgary ("The City") takes reasonable security safeguard measures to protect and manage personal information in its custody or under its control against such risks as unauthorized access, collection, use, disclosure, or destruction.

2.2. Following this administration standard will:

a) Foster public trust and confidence in The City through openness and transparency regarding the collection and management of personal information;

b) Provide direction with respect to the completion of Privacy Impact Assessment ("PIA") for new or modified projects, initiatives, programs, administrative practices or processes, or information systems that involve personal information;

c) Ensure sound management and decision making as well as careful consideration of privacy risks with respect to the collection, use, disclosure, or destruction of personal information as part of City programs and services; and,

d) Result in documented assurances that privacy was considered and reasonable steps were taken to identify, and either adequately addressed or, in the case of outstanding privacy issues, a mitigation strategy was developed.

3. DEFINITIONS

3.1. In this administration standard:

a) **"Collection"** means obtaining personal information from or about an individual, whether the information is recorded or not.

b) **"Completed"** means a PIA has undergone a thorough privacy risk analysis, formulating risk mitigations and has been issued a PIA report.

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

d) **"Custody"** means records that are in The City's possession and includes situations where the records belonging to a professional are kept by The City.

e) **"Disclosure"** means the publication, release, or sharing of Personal Information to another party or entity, external persons, and in some circumstances within The City.

f) **"Employee"** includes any person employed by The City or who performs a service for The City as an appointee, volunteer, or student, or under a contract or agency relationship with The City as per section 1(e) of the FOIP Act.

g) **"FOIP Program Administrator ("FOIP PA") and Alternate"** means the business unit representative(s) appointed to coordinate business unit activities supporting compliance and advancement of the Privacy Management Program.

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

- the individual's name, home or business address, or home or business telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
- the individual's age, sex, marital status, or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information, or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment, or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and,
- the individual's personal views or opinions, except if they are about someone else.

i) **"Privacy Impact Assessment" or "PIA"** means an analytical process to help identify and address potential privacy risks before the implementation of a project, initiative, program, administrative practice or process, or information system that involves personal information.

j) "**Project Team Members"** means individuals who are familiar with the project, initiative, program, administrative practice or process, or information system associated to the PIA.

4. APPLICABILITY

4.1. This administration standard applies to all Employees.

4.2. This administration standard does not apply to:

a) Elected Officials;

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

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

5. STANDARD

5.1. Employees are responsible for:

a) Initiating a PIA for new or modified projects, initiatives, programs, administrative practices or processes, or information systems that involve personal information;

b) Participating in PIAs by collaborating with FOIP Coordinator or delegate to identify and address potential privacy risks of:

i. Collection, use, and disclosure of personal information practices;
ii. Notification practices;
iii. Storage, security, retention, and destruction practices; and,
iv. Related personal information flows.

5.2. FOIP Program Administrators ("FOIP PAs") are responsible for:

a) Initiating privacy consultations and engagement between FOIP Coordinator or delegate and their business unit, including new or modified projects, initiatives, programs, administrative practices or processes, or information systems that involve personal information;

b) Supporting their business unit in implementing privacy protection measures; and,

c) Assisting their business unit with PIA by:

i. Facilitating completion of the PIA process and maintenance of business unit PIA reports;

ii. Responding to six-month PIA follow-up recommendations requests; and,

iii. Creating Personal Information Banks for completed PIAs, as needed.

5.3. Business Unit Managers are responsible for:

a) Ensuring that business unit is implementing privacy recommendations from PIA report, or in the case of outstanding privacy issues, ensuring that a mitigation strategy is developed.

5.4. FOIP Coordinator is responsible for:

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

b) Making decisions to forward complex PIA cases for review to the Office of Information and Privacy Commissioner ("OIPC") of Alberta;

c) Receiving and validating PIA submissions, including consulting with Project Team and PIA submitter and returning incomplete submissions with privacy guidance;

d) Conducting privacy risk assessments in accordance with best practices and in compliance with the FOIP Act by documenting identified risks, recommending controls to address, and advising conditions that should be met prior to project implementation;

e) Issuing, based on the privacy risk assessment findings, written report with recommended privacy risk mitigations;

f) Requesting follow-up reports from PIA submitters or business unit FOIP PA six months after issuing a PIA report;

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

h) Annually preparing and circulating to business unit FOIP PA an outstanding PIA recommendations report.

5.5. Project Team Members are responsible for:

a) Identifying a PIA submitter to submit the PIA on behalf of the project team and act as a conduit in communicating PIA results, associated privacy recommendations, and follow-up requests;

b) Completing a PIA in consultation with potential impacted business unit(s) including providing associated project documentation, such as:

   i. Project business case;

   ii. Risk value assessment;

   iii. Corporate cloud assessment;

   iv. Information sharing agreement;

   v. Third-party privacy policies or associated terms of use; and,

   vi. Flow charts and/or drawings of infrastructure and flows of information;

c) Alerting the FOIP PA and FOIP Coordinator or delegate of changes made to a project, initiative, program, administrative practice or process, or information system that involves personal information so that the existing or in-progress PIA can be reviewed;

d) Conducting an annual review of each PIA for multi-year projects to ensure information in the PIA reflects current practices and processes; and,

e) Implement privacy recommendations from PIA reports in a timely manner, as deemed appropriate, or in the case of outstanding privacy issues, implementing a mitigation strategy.

7. CONSEQUENCES

7.1 Employees who fail to adhere to this administration standard and any associated policy and procedures may result in disciplinary action in accordance with either the *Labour Relations Policy* or *Exempt Staff Policy*.

7.2 Employees who fail to comply with the duties imposed by the FOIP Act or otherwise act in contravention of the legislation may lead to penalties or offences under the FOIP Act.

8. HISTORY

Action	Date	Report Number	Description
New	March 22, 2024	n/a	Includes material from Privacy Impact Assessment policy rescinded as of December 18, 2023