Guideline
Privacy Impact Assessments

This guideline falls under *A1477 Data and Information Management Administrative Policy.*

Program Impacted	Civic Services *Edmontonians contribute to civic society and are engaged in promoting the quality of the community.* Technology & Data *The City of Edmonton's technology and data are leveraged to enable quality decision-making and enhance innovative service delivery.*
Approved By	Aileen Giesbrecht, City Clerk
Date of Approval	May 13, 2026
Approval History	N/A
Next Scheduled Review	May 13, 2027

Guideline statement

This guideline provides guidance on the necessary components and process of completing a Privacy Impact Assessment in accordance with the *Protection of Privacy Act* (POPA).

Scope

This guideline provides direction to all City of Edmonton departments undertaking new initiatives or significantly amending initiatives involving the collection, use or disclosure of personal information, non-personal data or data derived from personal information.

This guideline also provides recommendations to City of Edmonton employees, contractors, volunteers, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head. It applies to these parties whenever their work involves creating, collecting, receiving, accessing, using, disclosing, storing, maintaining, destroying or transferring City records and information. All individuals listed above are responsible for protecting the privacy and confidentiality of personal information in accordance with POPA.

Definitions

Common or integrated program or service means a program or service planned, administered, delivered, managed, monitored or evaluated by the City working collaboratively with one or more other public bodies, another public body working on behalf of the City or the City and one or more other public bodies.

Control means the capacity to manage and determine the use of a record or information.

Custody means to have physical possession of a record of information. For example, records stored in Google are under the City's control, but not in the City's custody because the City does not have physical possession of the records.

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.

Data matching means linking personal information between two or more databases or other electronic sources of information.

An *information flow diagram* is a visual map that shows how data will move in the initiative. It tracks where information comes from, where it goes and how it’s handled. These maps usually come with tables that explain exactly what data is being shared, when it is shared and the specific reasons for each step.

An *initiative*, for the purpose of this guideline, is 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. For clarity, this may include but is not limited to:

- implementation of new software or cloud services;
- a City program or service;
- public engagement, surveys and collection of feedback;
- modernization of existing process;
- workplace wellness programs; or
- predictive analytics.

Innovative technology, for the purpose of this guideline and the Privacy Impact Assessment (PIA) Standard, means a method, software, hardware, application or manipulation of personal information, data derived from personal information or non-personal data that is:

a) new to the City of Edmonton;
b) not previously used in the way it will be used in the initiative; or

c) is likely to be considered novel, new or innovative by the public.

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. This includes synthetic data.

Personal information means any recorded information about an identifiable individual, including but not limited to:

a) 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;
b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;
c) the individual's age, gender identity, sex, sexual orientation, marital status or family status;
d) an identifying number, symbol or other particular assigned to the individual;
e) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
f) information about the individual's health and health care history, including information about the individual's physical or mental health;
g) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
h) anyone else's opinions about the individual; and
i) the individual's personal views or opinions, except if they are about someone else.

Sensitive personal information means personal information that, if disclosed, could likely expose the subject to significant harm, such as:

a) bodily harm;
b) humiliation or damage to reputation or relationships;
c) loss of employment, business or professional opportunities;
d) identity theft;
e) negative effects on insurability;
f) negative effects to an individual's credit record; or
g) damage to or loss of property, other legal harms or financial losses.

The following types of personal information are automatically considered highly sensitive:

h) biometric information about an individual;
i) financial information about an individual; and
j) personal information respecting a minor, senior or vulnerable individual.

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.

Guideline specification

A Privacy Impact Assessment (PIA) is a step-by-step process used to analyse a practice, program, project or service (initiative) to identify and address individual privacy risks. A PIA is required when the initiative in question collects or uses personal information and meets the requirements in the *Privacy Impact Assessment Standard*. It must be completed and submitted to the Office of the Information and Privacy Commissioner (OIPC) by the Access and Privacy Head/City Clerk before the program, service or initiative can be launched, as per the requirements in *the Protection of Privacy (Ministerial) Regulation*. Business areas should start the PIA process far enough in advance to allow time for completion of City endorsement and approval processes.

Collecting information required to begin a PIA Intake Form

Business areas need to collect or compile the following information about the initiative before beginning the PIA process:

- a clearly defined scope for the initiative, including its relationship to other existing initiatives;
- the rationale, including identifying the problem the initiative addresses and the City's mandate with regard to the initiative;
- what personal information and non-personal data will be collected, used and/or disclosed, as well as the security classification of that data;
- business area governance regarding the collection, access, use, disclosure, protection and stewardship of the personal information involved in the initiative.
- if involving a common or integrated program or service:
    - what parties are involved; and
    - the roles and responsibilities of each party (precise requirements are in the *Privacy Impact Assessment Administrative Standard*);
- if using a service where vendors will have access to the information:
    - the vendors involved; and
    - the contractual controls regarding personal information.

Determining if a PIA is required

Corporate Access and Privacy assists business areas in determining if a PIA is required for an initiative by evaluating PIA Intake Forms completed by the business area. Business areas determine whether their initiative involves personal information, then complete and submit a PIA Intake Form (internal use only). The Privacy team evaluates the information received from the business area to determine whether a PIA is required, then informs the business area of the determination.

Completing the PIA

Business area responsibilities

The business area is responsible for fully completing the parts of the PIA template labelled "To be completed by the Business Area." These parts cover information about the initiative, including:

- a complete information flow diagram with supporting tables to account for the personal information involved in the initiative accurately;
- whether the initiative is part of a common or integrated program or service;
- whether there is data matching as part of the initiative;
- how custody and control of the personal information works under the initiative; and
- whether there is any creation, use or disclosure of non-personal data as part of the initiative.

In some cases, business areas will need to engage resources in Open City and Technology to adequately describe technology solutions used in their initiatives.

The business area is responsible for reviewing the PIA draft to confirm it is accurate and complete before submitting it to Corporate Access and Privacy (CAP).

CAP responsibilities

The assigned Privacy Analyst or Advisor, advised by the Privacy Manager, will review the PIA draft to determine the collection, use and disclosure authorities under POPA. CAP will also confirm that it:

- is coherent;
- adequately documents the collections, uses and disclosures of personal information; ;
- contains all necessary information and attachments; and,
- meets all other requirements of the Act and Regulations.

The assigned Privacy Analyst or Privacy Advisor will also fully complete the parts of the City's PIA template labelled "To be completed by CAP."

Interested party responsibilities

There may be different business areas that need to be consulted about the PIA. The business area and CAP will identify the interested parties collaboratively as the template is completed.

- *Corporate Information Security Office (CISO)* - For initiatives involving a new or significantly changed technology solution, or where any City information will be in the custody of a service provider, CISO will review and confirm if the initiative is compliant with the City's Cybersecurity Standards.
- *Legal Services* - For initiatives involving legislative authorities in addition to POPA and ATIA, Legal Services will confirm that the legislative authorities and responsibilities are accurately described in the PIA. This will typically involve the business area's lawyer in consultation with CAP's lawyer, as needed.

- *Department Records Advisors* - For initiatives involving the creation of new record types, the Department Records Advisor (DRA) will review and confirm that the retention of records associated with the initiative are described accurately in the PIA document.
- *Other City Departments* - There may be other interested parties depending on the nature of the initiative. For example, if multiple business areas are involved in an initiative, one is designated the primary business area, and the other areas are designated as interested parties. These interested business areas are responsible for reviewing and ensuring the content is accurate where it pertains to their roles and responsibilities.

Confirming PIA Accuracy and Compliance

Once the PIA draft is finalized, it will be circulated to the following parties, as appropriate:

- *Corporate Information Security Office (CISO)* - reviewing and confirming compliance with cybersecurity standards.
- *The business area's lawyer, Legal Services* - reviewing and confirming compliance with other legal requirements.
- *Manager or Director, Corporate Records and Information Management* - confirming compliance with classification and retention schedules.
- Any other parties identified as appropriate during drafting.
- *Branch Manager of the responsible business area* - formally confirming overall accuracy of the initiative and accepting risk and mitigations as described.
- *Director, Corporate Records, Information Management, Access and Privacy* - formally confirming compliance with POPA and readiness to submit to the OIPC or determining if the PIA should go to the Access and Privacy Head/City Clerk for confirmation.
- *Access and Privacy Head/City Clerk, The Office of the City Clerk* - formally confirming compliance with POPA for initiatives with a significant impact and readiness to submit to OIPC, if deemed required. Formally submitting the PIA.

Submitting the PIA to the OIPC

Once formally complete, the Access and Privacy Head/City Clerk will submit the PIA to the Office of the Information and Privacy Commissioner (OIPC) for review and comment. Once the PIA has been submitted, the initiative may commence. This is effective as of June 11, 2026.

If the OIPC has questions about the PIA submission, CAP will work with the responsible business area to answer the questions. Once a formal comment from the OIPC is received, CAP will prepare a briefing note that includes the OIPC comment and any supporting analysis for the responsible branch managers to consider.

Compliance

All City of Edmonton employees, contractors, volunteers, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head are responsible for maintaining the privacy and confidentiality of information in accordance with POPA. Branch managers are accountable for ensuring that privacy practices within their branches comply with legislation and City of Edmonton policy tools, including the *Corporate Records and Information Management Accountability Model (RASCI)*. Failure to comply with this standard could result in the loss of personal information, damage to the City of Edmonton's reputation, costs and fines, increased legal risk, information breaches and complaints from the public.

References and Supporting Resources

Legislation

- *Protection of Privacy Act, SA 2024, c P-28.5*
- *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025*
- *Protection of Privacy Regulation, Alta Reg 132/2025*
- *City Administration Bylaw, Bylaw 16620*
- *A1477 Data and Information Management Administrative Policy*

Supporting Resources

- City of Edmonton Delegation of Authority Order
- Corporate Information Management Glossary of Terms
- Privacy Impact Assessment Administrative Standard
- Privacy Impact Assessment Intake Form
- Privacy Impact Assessment Template