Privacy Management Program Charter

The City of Edmonton Privacy Management Program is designed to assist the City of Edmonton in meeting its legislative requirements by assuring compliance with the *Protection of Privacy Act (POPA)*, related regulations, corporate mandates, ethical standards and municipal bylaws. The City Clerk serves as the privacy officer of the Privacy Management Program, and Corporate Access and Privacy (CAP) within the Office of the City Clerk administers the program.

The Privacy Management Program provides coordination for corporate privacy tools, training, privacy impact assessments and privacy incidents.

All employees, contractors, volunteers, Council Committee members and individuals for whom the City Clerk acts as the Access and Privacy Head in the City of Edmonton are responsible for maintaining personal privacy and adhering to corporate policy tools. However, accountability ultimately rests with branch managers.

Corporate Privacy Management Governance

Corporate privacy management at the City uses a collaborative governance model that balances centralized oversight with departmental responsibility. At the core of this program is the Office of the City Clerk. The City Clerk has delegated authority to set rules for the collection, use, disclosure, retention, security and disposition of personal information and to ensure that individual rights are protected through alignment with POPA. For security arrangements, the City Clerk works in tandem with the Open City & Technology (OCT) branch, which implements the technical measures necessary to safeguard data. By leveraging the City Clerk and OCT's expertise, the City maintains a robust privacy program in which roles are clearly defined, from high-level delegation to the daily management of information security and disclosure.

The Privacy Management Program (PMP) is built on clear legislation and internal rules that keep the City of Edmonton transparent and accountable. At the highest level, the *Municipal Government Act* (MGA) provides broad statutory authority for the City’s governance and administration. At the same time, POPA serves as the specific legislative framework for municipalities on governing the collection, use and disclosure of personal information. This legal mandate is set out in *Bylaw 16620, the City Administration Bylaw*, which

empowers the City Manager to establish systems to enable City operations. Internally, *Administrative Policy A1477 Data and Information Management* sets the corporate standard for treating information as an imperative asset that must be protected throughout its lifecycle. Finally, the *Privacy Administrative Procedure and its subordinate policy tools* provide both an overview and implementable rules that translate into consistent, measurable practices for all city employees across all departments.

Roles, Responsibilities and Accountabilities

Privacy Management Program

The Privacy Management Program includes the roles and responsibilities laid out in Table 1.

Role	Key Responsibilities
City Clerk	Holds full delegated authority under POPA. This role provides mandatory policy concurrence for information security arrangements and high-level decisions regarding sensitive data disclosures, research conditions and the criteria for disclosing information during emergency situations.
Director, Corporate Records, Information Management, Access and Privacy	Provides strategic leadership and coordination for the Corporate Records, Information Management, Access and Privacy section in the Office of City Clerk. Reporting to the City Clerk, the Director has specific authorities in the delegation order, ensures corporate alignment and serves as a point of escalation for the Privacy Manager.
Branch Manager, Open City and Technology (OCT)	Ensures the effective implementation and maintenance of security arrangements to protect personal information, in collaboration with the Office of the City Clerk. Oversees staff who provide technical expertise for Privacy Impact Assessments.
Privacy Manager	Manages the Privacy team and the daily operations of the Privacy Management Program. This role serves as the senior privacy expert and is responsible for drafting policies, assigning work, refining program tools and addressing privacy risks. Acts as the first escalation point for Privacy Analysts and Advisors.
Privacy Advisor	Leads privacy incident response and investigations and stewards complex or high-risk Privacy Impact Assessments (PIAs) from intake to OIPC submission. Provides expert compliance consultations to various business areas.

Role	Key Responsibilities
Privacy Analyst	Facilitates business area compliance through consultations and the stewardship of PIAs from intake to OIPC submission. Processes personal information correction requests and provides backup support where required.

Table 1: Roles and responsibilities within the Privacy Management Program

Privacy across the Corporation

Roles across the broader corporation have specific privacy responsibilities as listed in Table 2.

Role	Key Responsibilities
Branch Managers	Accountable for ensuring branch-level adherence to privacy legislation and City of Edmonton policies. This includes implementing and maintaining the *Corporate Records and Information Management Accountability Model* (RASCI) and ensuring compliance with the Access to Information and Protection of Privacy Chart within their respective business areas.
All Staff	Responsible for maintaining the privacy and confidentiality of information in strict accordance with POPA. This mandate applies to all City employees, contractors, volunteers, Council Committees, and any individuals for whom the City Clerk acts as the Access and Privacy Head.

Table 2: Corporate roles and responsibilities

Program Components

In alignment with the privacy management program requirements laid out in the *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025*, the City's Privacy Management Program includes the following elements.

Privacy Incident Response

Privacy incidents include both privacy complaints and potential privacy breaches. A privacy breach is an incident where personal information is collected, accessed, used, disclosed or deleted in a manner that is not authorized under the Protection of Privacy Act (POPA).

When an incident is reported, either by a City business area or a member of the public, the Corporate Access and Privacy leads the intake, review and response.

Standards and Guidelines

Privacy Incident Risk Assessment and Notification Standard
Privacy Incident Response Guideline

Personal Information Correction

Members of the public may contact Corporate Access and Privacy if a City record requires correction to their personal information. Personal information updates, such as surname changes, are implemented by the business areas responsible for the information. Information will also be provided to direct the public to alternate ways to correct their information, providing efficiency options and improved accessibility.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a step-by-step process used to analyse a new or significant change to an existing practice, program, project or service (initiative) in order to identify and address individual privacy risks. A City business area initiates a PIA 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) before the initiative can be launched. This is effective as of June 11, 2026.

Corporate Access and Privacy works with business areas to determine whether a PIA is needed for an initiative, provides guidance on completing the required forms, and coordinates submissions and responses to the OIPC. Responses from the OIPC to PIA submissions are shared with the Branch Managers of the business area(s) for consideration.

Standards and Guidelines

- Privacy Impact Assessments Standard
- Privacy Impact Assessments Guideline

Corporate Privacy Guidance

Corporate Access and Privacy guides business areas on how to collect and protect personal information. CAP also provides standards for managing non-personal data.

Responsibility for providing reasonable security arrangements for the protection of personal information in automated systems and for monitoring these systems is delegated to the Branch Manager, Open City and Technology and the City Clerk. Operationally, digital information security arrangements are managed by the Corporate Information Security Office.

Standards and Guidelines

- Consent to Use or Disclose Personal Information Standard
- Creation and Protection of Non-personal Data Standard
- Data Collection Statements Standard

Generative AI Standard
Non-personal Data Guideline

Mandatory Corporate Privacy Training

The City of Edmonton provides mandatory *Privacy and Access to Information* training for all employees. Training covers:

- An introduction to access and privacy legislation
- Employee roles and responsibilities
- Instructions for reporting a privacy incident or complaint
- Explanation of how to respond to a records search request
- Contact information for CAP in the Office of the City Clerk.

CAP is also available to provide business-area-specific privacy training upon request.

Personal Information Safeguards

Information Security Classifications

City of Edmonton employees, volunteers, contractors, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head must assign a security classification level to all personal information, data derived from personal information and non-personal data in its custody or under its control. The security classification level assigned to personal information will reflect its sensitivity.

Default information security classifications are listed in the *C*ity of Edmonton Classification and Retention Schedule for all record types. See the Records Management for Physical Records Administrative Guideline for recommendations on filing physical records by security classification.

Standards and Guidelines

City of Edmonton Classification and Retention Schedule
Physical Records Management Administrative Guideline

Additional Safeguards

- Administrative safeguards, such as setting file permissions, are overseen by Corporate Records and Information Management (CRIM) in the Office of the City Clerk. CRIM provides the corporation with the minimum requirements for securely managing personal information in both physical and digital environments. These safeguards are specified in a number of the lifecycle management policy tools under the Data and Information Management Administrative Policy A1477. Individual business areas

are responsible for detailing administrative safeguards for their information in documented processes.

- Physical safeguards, such as locking file cabinets, are also prescribed by Corporate Records and Information Management (CRIM) in the Office of the City Clerk. The minimum physical safeguards are detailed in the *Records Management for Physical City Records Administrative Guideline*.
- Technical safeguards are captured in the City of Edmonton Corporate Information Security standards.

Program Review, Assessment and Update

The Director of Corporate Records, Information Management, Access and Privacy will review the Privacy Management Program every three years at a minimum or as needed due to legislative, regulatory or corporate changes and recommend amendments to the City Clerk as necessary to ensure the program remains complete, compliant and up-to-date.

Privacy Management Program Charter Approvals

Director, Corporate Records, Information Management, Access and Privacy	April 16, 2026 Date

Access and Privacy Head and City Clerk	April 16, 2026 Date

Procedure
Privacy

This procedure 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

Procedure Statement

This procedure is to be used by all City of Edmonton employees to ensure compliance with the *Protection of Privacy Act (POPA)* and to establish our commitment to protecting all personal and non-personal information, as well as data derived from personal information, that the City collects, creates, uses or discloses.

Scope

This procedure applies 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.

Procedure Description

This procedure provides an introduction to the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy:*

> "[The] Privacy (P) [function] maintains individual privacy, ensures compliance with the *Protection of Privacy Act* and applies high ethical and technical standards with regards to privacy principles."

These privacy principles include:

- *Careful use of personal information:* The City of Edmonton will use only the personal information that is absolutely necessary for research, analysis or program and service design and delivery. In each instance, the City will use the least amount of personal information necessary to achieve the purpose. Wherever possible, the City of Edmonton will use non-personal data. The City of Edmonton will not sell personal information in any circumstance or for any purpose, including marketing and advertising.
- *Clear sharing regulation:* The City of Edmonton will have clear rules for when and how to share information with other public bodies for purposes authorized by POPA.
- *Transparent use for automated systems:* The City of Edmonton will notify individuals if their information is used in an automated system to generate content or make decisions, recommendations or predictions.
- *Proactive analysis and mitigation of potential privacy impacts:* The City of Edmonton will ensure that whenever a system involving personal information is being developed or substantially changed, the City will do a privacy impact assessment to analyse potential impacts and remain compliant with POPA.
- *Immediate notification of parties affected by privacy incidents:* The City of Edmonton will notify individuals about any potential privacy breach where there is a real risk of significant harm.

Definitions

Access and Privacy Head of the Public Body means the City Clerk, to whom the City Manager, as the head of the public body, has delegated all powers, duties, and functions under the *Access to Information Act* (ATIA) and the *Protection of Privacy Act* (POPA), except the power to delegate under section 87 of ATIA and section 55 of POPA.

Data derived from personal information means data created by data matching 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.

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. It 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.

Procedure Specification

City of Edmonton employees, contractors, volunteers, Council Committees and any individuals for whom the City Clerk acts as the Access and Privacy Head are the protectors of the City's information, including:

- Personal information
- Data derived from personal information
- Non-personal data

They are required to:

- Respect the confidentiality of personal information
- Comply with the City's and their branch's information control and security systems
- Report any privacy incidents to their immediate supervisor or in accordance with the Privacy Incident Risk Assessment and Notification Standard.

Within their branches, branch managers are accountable for ensuring that privacy is managed and complies with POPA and corporate policy tools. This includes:

- Providing privacy strategies, goals, procedures, standards and guidelines for the collection, use and disclosure of personal information that applies to their lines of business

- Ensuring that managers, supervisors and employees receive appropriate privacy training, thereby providing adequate information to all employees with respect to their responsibilities under POPA
- Being responsible for personal information controls, security systems and decisions about the management of personal information
- Ensuring that a Privacy Impact Assessment is included in the initial plan stage for new or updated services, projects or programs and that resources are assigned to complete the Privacy Impact Assessment
- Ensuring that requests for correction of personal information are implemented within their records and systems
- Supporting a culture of privacy compliance and respect for personal information

The City Clerk is the privacy officer for the City of Edmonton, ensuring that the City collects, uses and discloses an individual's personal information only for authorized purposes. The City Clerk oversees the privacy management program, which provides corporate direction on how the City will comply with POPA. The *Privacy Management Program Charter* lays out the program's purpose, goals and components.

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)* and the *Access to Information and Protection of Privacy Authority Chart*. Failure to comply with this guideline 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 Management Program Charter

Standard
Privacy Incident Risk Assessment and Notification

This standard 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

Standard Statement

This standard governs responses to privacy incidents as required by the *Protection of Privacy Act (POPA)* s 10 and *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025* s 4.

This standard falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

This standard applies 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

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. It 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.

A *privacy incident* is any potential unauthorized collection, access, use, disclosure or destruction of personal information or non-personal data. This may include complaints, observations or reasonable suspicion of unauthorized activity regarding personal information or non-personal data or any other breach of POPA.

A *privacy breach* is a confirmed unauthorized collection, access, use, disclosure or destruction of personal information or non-personal data.

Significant harm means bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

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.

Standard Specification

In the event of a privacy incident, the City of Edmonton will conduct an assessment to determine if a real risk of significant harm exists, which includes, but is not limited to, assessing:

a) if there is a reasonable basis to believe that the personal information has been misused or will be misused
b) whether the incident occurred as a result of malicious intent
c) the sensitivity of the personal information involved in the incident
d) any steps taken to reduce the risk of significant harm

In the event that the privacy incident represents a risk of significant harm to an individual under *Alta Reg 143/2025* S4(2), the City of Edmonton will give written notice, without unreasonable delay, to the individual(s) whose personal information was involved, the Information and Privacy Commissioner and the Minister responsible for POPA.

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)* and the *Access to Information and Protection of Privacy Authority Chart*. Failure to comply with this guideline 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
Council Committees Bylaw 18156
Agencies, Boards, Committees and Commissions Council Procedure
A1477 Data and Information Management Administrative Policy

Supporting Resources

City of Edmonton Delegation of Authority Order
Corporate Information Management Glossary of Terms

Corporate Records and Information Management Accountability Model (RASCI)

Guideline
Privacy Incident Response

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 an overall framework for responding to privacy incidents, including intake, containment, notification, regulatory investigation, communications and OIPC inquiries.

This guideline falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

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, that are:

- are affected by or responsible for a privacy incident or
- have submitted or received a privacy complaint.

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 the *Protection of Privacy Act* (POPA)

Definitions

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. It 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.

Privacy incident means any potential unauthorized collection, access, use, disclosure or destruction of personal information or non-personal data. This may include complaints, observations or reasonable suspicions of unauthorized activity regarding personal information or non-personal data or any other potential breach of POPA.

A *privacy breach* is a confirmed unauthorized collection, access, use, disclosure or destruction of personal information or non-personal data.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

Guideline Specification

This guideline provides an overview of privacy incident response procedures, as well as a high-level overview of the roles of:

- Access and Privacy Head/City Clerk
- Corporate Access and Privacy
- Affected business areas
- Employee Services
- Open City and Technology
- Corporate Communications
- Legal Services

Intake

When the public or an employee has concerns regarding collection, use, access or disclosure of personal information, they can submit a privacy complaint to CAP via email, the Privacy Incident Reporting Form (if an employee) or the Public Privacy Incident Reporting Form. Once a complaint is received, the Privacy Manager assigns it to a Privacy Advisor. The Privacy Advisor logs the incident in the same manner as Internal Reports, then sends an acknowledgement to the complainant.

Containment

When a privacy incident occurs, containment is the most time-sensitive step. The type of containment required depends on the type of incident - see Table 1: *Examples of typical privacy incidents (not an exhaustive list)*.

Type of Incident	**Containment Step**
Correspondence was sent to an unintended recipient by post.	Ask the recipient to either: ● send the correspondence back or ● shred and confirm destruction.
Correspondence was sent to an unintended individual via email.	Ask the recipient to delete the email and its attachment and confirm deletion.
An employee received unauthorized access to internal City folders.	Revoke access.
An employee accessed files or City systems for a purpose other than their work.	Revoke access.

Generally, the business area will lead containment with assistance from CAP. OCT may be tasked with containing specific incidents, including cyberattacks. Although total containment isn't always possible, the City will use every reasonable effort to mitigate the impact as quickly as possible.

Notification

Branch Managers are notified when CAP intends to contact their staff regarding a privacy incident. This occurs if the business area was (in)directly involved in or affected by the incident. Other individuals who may be affected by the incident (e.g. their personal information was disclosed without authorization) may also receive a notification depending on the level of risk identified.

Incident Severity and Reporting

- *Low-risk Incidents*: Low-risk incidents aren't complex, don't meet Real Risk of Significant Harm (RROSH) criteria and do not require a regulatory investigation, such as accidentally emailing the wrong recipient who is also a City employee (and bound by the code of conduct)
    - Branch managers receive only a "for awareness" notice once the file is closed from CAP. No further action is needed.
    - A Privacy Advisor may still recommend *courtesy notification*s to the affected individuals to protect the City's reputation or ensure fairness. The final decision to proceed with the notification rests with the branch responsible for the incident.
- *High-risk Incidents*: High-risk incidents are more complex, where Corporate Access and Privacy (CAP) has identified potential RROSH and the incident requires a regulatory investigation:
    - Branch Managers are notified by CAP that a regulatory investigation will commence early in the process.
    - If RROSH criteria were met:
        - The responsible branch or the branch with an existing relationship with the affected individuals must notify them. CAP will provide language support. If required, Communications will be engaged to provide support for this step.
        - CAP will prepare formal notifications for the OIPC and the Minister of Information and Technology and Legal Services. The Access and Privacy Head/City Clerk sends these notifications.
    - If RROSH criteria were not met, a Privacy Advisor may still recommend *courtesy notifications* to the affected individuals to protect the City's reputation or ensure fairness. The final decision to proceed with the notification rests with the branch responsible for the incident.

Regulatory Investigation

The goal of a regulatory investigation is to determine the following:

1. Did a breach of POPA (an unauthorized collection, use or disclosure of personal information or non-personal data) take place?
2. If yes, what were the root causes and contributing factors of the breach?
3. Did the City have adequate security measures in place to prevent the unauthorized collection, use or disclosure of personal information or non-personal data?
4. What, if any, recommendations could be made to prevent a recurrence of a similar incident?

Investigative actions are customized for each case, determined by the nature of the incident and the most accurate information sources, balanced with practical necessity. The following activities may be deployed as part of an investigation:

- Collection of evidence of the breach, which may include, but is not limited to, pictures, emails and spreadsheets.
- Proof of containment, such as an email confirming deletion from an unintended recipient.
- Reviews of policies, procedures, manuals, training or other instructive material.
- Interviews with individuals with knowledge of the incident or the relevant business areas. Formal interviews are conducted in conjunction with Employee Services. Informal interviews will be led by CAP.
- Reviews of software audit logs or security records, in conjunction with OCT.
- Meetings and/or correspondence with complainants to understand their concerns and any evidence they wish to bring forward regarding a potential breach of POPA.

Communication of Findings

At the conclusion of an investigation, branch managers are provided with findings about the events in their branches in a variety of ways:

- *Incidents that do not require an investigation (low risk, low complexity):* Branch managers are notified via email (see Notifications, above).
- *Incidents requiring an investigation:* Branch managers receive a briefing note at the conclusion of the investigation detailing findings for their consideration, including:
    - whether any unauthorized collections, uses or disclosures took place
    - containment details, if applicable
    - whether regulatory body or courtesy notifications took place
    - analysis of the cause of the incident and
    - recommendations to prevent similar incidents from happening in the future
- *Major incidents:* CAP prepares a longer-form findings report, reviewed and approved by the Access and Privacy Head/City Clerk. The Access and Privacy Head/City Clerk or delegate (Director, CRIMAP) circulates it to deputy City managers, branch managers and other impacted executive leadership.

- *Incidents reported to the OIPC:* If the incident report details change after the initial report, the Access and Privacy Head/City Clerk or delegate (Director, CRIMAP) will email the updated information to the OIPC. Before reporting any completed recommendations to the OIPC, CAP will coordinate with the relevant business areas to confirm they have been fully implemented.

OIPC Investigations and Inquiries

Initiation of Reviews

The Office of the Information and Privacy Commissioner (OIPC) may investigate reported privacy incidents at their discretion. These reviews may be triggered by the formal notification from the City, a formal complaint from an affected individual or a special investigation initiated directly by the Commissioner. The OIPC assigns one of their Senior Information and Privacy Managers (SIPM) for these investigations.

Mediation/Review Phase

CAP is responsible for coordinating and responding to all OIPC matters during the mediation or review stage. CAP also coordinates and responds to special investigations. To ensure a comprehensive response, CAP collaborates with the originating business areas and all relevant stakeholders.

Inquiry Phase

If a matter remains unresolved following mediation or review, the OIPC may conduct a formal inquiry. The Commissioner may assign an Adjudicator to perform this role. Information supplied during the mediation and review stage is not considered during inquiry. At this stage:

- Legal Services is responsible for leading the response.
- CAP transitions the file to the assigned City solicitor and provides ongoing support.

Collaboration remains a priority to ensure that all prior actions and incident details are accurately and thoroughly documented in the City's formal submission.

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)* and the *Access to Information and Protection of Privacy Authority Chart*. Failure to comply with this guideline 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 Incident Report Form (internal)

Privacy Incident Report Form (public-facing)

Standard
Privacy Impact Assessments

This standard 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

Standard Statement

This standard governs the requirements for a Privacy Impact Assessment (PIA) as required by the *Protection of Privacy Act (POPA)* s 26 and *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025* s 7.

This standard falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

This standard applies 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.

Innovative technology, for the purpose of this standard and the PIA Guideline, 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.

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.

Reasonable security arrangements mean administrative, physical and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of a public body that:

a) are appropriate and proportional to the security classification level of the information or data; and
b) in the case of non-personal data, ensure, to the extent possible, that the identity of an individual who is the subject of the non-personal data cannot be re-identified from the data.

Standard Specification

Effective June 11, 2026, business areas must prepare Privacy Impact Assessments (PIAs) for new practices, programs, projects or services ("initiatives") or for substantial changes to existing ones, where:

a) the *Protection of Privacy (Ministerial) Regulation* requires a PIA to be submitted to the Office of the Information and Privacy Commissioner (OIPC);
b) unauthorized access or disclosure of the personal information involved in the initiative presents a real risk of significant harm (RROSH); or
c) the Information and Privacy Commissioner requests a copy of a PIA under section 27(1)(j) of POPA.

The level of detail included in the PIA shall match the complexity of the project.

The PIA will include:

- a description of the project;
- a summary of the purpose of the collection, use or disclosure of personal information;
- the types of personal information that will be collected, used or disclosed;
- the reasonable security arrangements in place to protect that personal information;
- the legal authority for the collection, use or disclosure of the personal information;
- any privacy risks and mitigation strategies respecting the personal information;
- any administrative, physical or technical safeguards in place to protect the personal information, including how the personal information will be securely transmitted, matched or linked by the City of Edmonton, if applicable;
- the procedures to ensure accuracy and completeness of the personal information used; and
- if two or more public bodies are involved, a clear governance structure respecting the responsibilities and accountability of each party.

These PIAs shall be provided to the Information and Privacy Commissioner before implementation of the initiative when a practice, program, project or service:

- involves highly sensitive personal information;
- involves the personal information of a substantial portion of the population;
- involves data matching between two or more public bodies;
- involves programs or services operated in cooperation with another public body or organization; or
- involves the development or use of innovative technology.

PIAs will also be provided upon request from the Commissioner.

A Privacy Impact Assessment conducted by any City of Edmonton business area will use the instructions and questionnaire provided by the Office of the Information and Privacy Commissioner (OIPC).

Corporate Access and Privacy in the Office of the City Clerk will advise business areas on the preparation of PIAs and conduct reviews to ensure they are complete and compliant with both City and regulatory requirements before approval. Where appropriate, the business area will engage the Corporate Access and Privacy team, the Corporate Information Security Office, Legal Services, Corporate Records and Information Management and any other corporate stakeholder necessary to complete the PIA to corporate standards, as defined in the Privacy Impact Assessment Standard Operating Procedure.

Where required by the POPA Regulation, the Office of the City Clerk will submit any PIAs to the Office of the Information and Privacy Commissioner before implementation of the initiative.

Common and Integrated Programs and Services (CIPS)

A PIA must be completed for all common or integrated programs or services (CIPS), as defined above, entered into by the City of Edmonton with other public bodies, under section 7 of the *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025*. The agreement establishing the City's involvement in a common or integrated program or service must contain the necessary information to complete the required PIA.

The CIPS agreement must:

- describe how the public bodies will comply with the *Protection of Privacy Act.*
- clearly define the governance structure of the common or integrated program or service, including the roles, activities and purposes of each public body's involvement.
- outline each public body's responsibilities regarding the personal information and non-personal data involved, including:
    - what types of personal information and non-personal data each public body is responsible for; and
    - who has custody and control of the personal information and non-personal data.

Each public body must be responsible for the personal information and non-personal data under its custody and control, including:

- managing retention schedules;
- processing Access to Information Requests;
- responding to a privacy incident or complaint related to the program;
- answering any questions from the public regarding their personal information, including how it is governed and protected; and
- ensuring adequate security measures to protect personal information and non-personal data.

The agreement, memorandum of understanding (MOU) or other governing document between public bodies must be finalized, or at least substantially and reliably worked out with respect to the above responsibilities, before proceeding with the PIA.

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
- Office of the Information and Privacy Commissioner (OIPC): Privacy Impact Assessment Resources
- Privacy Impact Assessment Guideline
- Privacy Impact Assessment Template

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

Standard
Consent to Use or Disclose Personal Information

This standard 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	Novmeber 13, 2026

Standard Statement

This standard governs the collection of consent to use or disclose personal information as required by the *Protection of Privacy Act (POPA)* s 12 and *Protection of Privacy Regulation, Alta Reg 132/2025* s 2.

This standard falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

This standard applies 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

Consent means a recorded, voluntary and clear agreement to a course of action.

Electronic consent means a consent provided by electronic means, including being created, recorded, transmitted or stored in digital form by electronic means, or by other means that have similar capabilities for creation, recording, transmission or storage.

Electronic signature means electronic information that an individual creates or adopts in order to sign a record that is in, attached to or associated with the record.

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.

Standard Specification

Under POPA, the City will rely on consent to use or disclose personal information **only** if the individual whose personal information is involved was informed of this use or disclosure at the time of consent. The City will rely only on consent to use or disclose personal information when the consent is freely given and the individual has been informed of any adverse consequences associated with their decision.

The City of Edmonton will use or disclose personal information only to the extent necessary to carry out the purpose stated in the original consent and not for any other purpose.

Providing Consent to Use or Disclose Personal Information

In all cases where consent is the authority to use or disclose personal information, there must be a record created of the consent that is accessible in the event of a dispute or complaint. The record of consent must be maintained for the life of the record being used or disclosed.

Written Consent

Written consent is accepted in all instances where consent is the authority to use or collect personal information. Written consent must include the consenting individual's signature.

Electronic Consent

Electronic consent can be used when written consent is unavailable or inaccessible to the individual who must provide consent.

Electronic consents are considered valid if:

- It is accessible and readable for subsequent reference.
- It is retained for the applicable retention period.
- It captures that consent was provided by the consenting individual.
- It demonstrates that the record has not been altered since consent was provided.
- It allows for the individual giving the consent to be identified.
- The association of the electronic signature with the consent is reliable for the purpose for which consent is given.

Oral Consent

Oral consent will be accepted from individuals who, by reason of disability, impairment or other lawful reason, can legally provide consent but are unable to sign a document. Consent will be obtained orally, with a third-party individual signing on their behalf or with an audio recording of the consent. The employee collecting the consent form will document that consent was provided orally.

Business areas will determine on a case-by-case basis which consent options will be offered for a particular use or disclosure. The business area must explicitly state which forms of consent they will accept.

Implied Consent

If an individual voluntarily provides personal information to the City for a specific purpose, but does not explicitly provide consent, the City will use and disclose the provided information as is reasonable for that person under the principle of implied consent. Implied consent only allows the City to use or disclose the personal information as is necessary to fulfill the purposes for which it was provided.

Withdrawing Consent to Use or Disclose Personal Information

Under POPA, individuals have the right to change or withdraw their consent to use or disclose their personal information. When the City of Edmonton receives notification from an individual that they wish to withdraw their consent, the City will:

1) Inform the individual of the likely outcomes if they are not readily apparent. In the case of disclosure, the City will inform the individual that the withdrawal will affect future disclosures but will not reverse disclosures already made.
2) Confirm with the individual that, now that they know the potential outcomes, they still want to withdraw their consent.
3) Record the withdrawn consent.
4) Once confirmed, stop collecting, using or disclosing the individual's personal information.
5) Maintain the record of withdrawal in accordance with the City of Edmonton Classification and Retention Schedule.

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, unnecessary 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
Electronic Transactions Act, SA 2001, c E-5.5
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

Standard
Creation and Protection of Non-personal Data

This standard 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

Standard Statement

This standard governs the creation and protection of non-personal data as required by the *Protection of Privacy Act (POPA)* S21-24 and *Protection of Privacy (Ministerial) Regulation, Alta Reg 143/2025* S5.

The following are not considered non-personal data and do not fall under this standard:

- the redaction of information from a record as part of a response to an access to information request,
- the creation of a record without identifiable personal information using unstructured data, which may have contained personal information, for routine or proactive disclosure only, and
- the production of a report, summary or other publication containing non-personal data that is in aggregate or statistical form.

Scope

This standard applies 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

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.

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.

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.

Structured data means data that resides in fixed fields (rows and columns) within a record or file in a database.

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.

Unstructured data means information that does not reside in fixed fields (rows and columns) of a database.

Standard Specification

The City of Edmonton will create non-personal data only for:

a) research and analysis, and/or
b) planning, administering, delivering, managing, monitoring or evaluating a program or service.

This non-personal data will be created in accordance with generally accepted best practices and any prescribed requirements set out in POPA regulations.

When creating non-personal data, the City of Edmonton will use only data already under its custody and control. At the time of creation, the City of Edmonton will record the following:

a) a description of the personal information or data derived from personal information used to create the non-personal data,
b) the purpose of the non-personal data,
c) the method used to create the non-personal, and
d) assessment results that confirm individuals cannot be identified or re-identified from the non-personal data.

The record of the above must be maintained for the life of the non-personal data and in accordance with the City of Edmonton Classification and Retention Schedule.

The City of Edmonton will disclose non-personal data to an individual outside of the corporation only for the following purposes:

a) research and analysis, and/or
b) planning, administering, delivering, managing, monitoring or evaluating a program or service.

Any non-personal data to be disclosed to an individual outside of the corporation will only be released upon the signature of an agreement specifying:

a) security and confidentiality requirements,
b) the prohibition of any actual or attempted re-identification of the non-personal data,
c) the prohibition of further disclosure of the non-personal data without the express written consent of the City of Edmonton, and
d) the requirement to destroy the data when it is no longer needed.

Agreements may be long-form written documents, but checking a box to agree to terms and conditions may also constitute such an agreement.

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, unnecessary 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

Standard
Data Collection Statements

This standard 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

Standard Statement

This standard governs the creation and use of data collection statements as required by the *Protection of Privacy Act (POPA)* S5.

Scope

This standard applies 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 the *Protection of Privacy Act* (POPA).

Definitions

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.

Standard Specification

A data collection statement must include the following elements:

1. The purpose for which the personal information is collected.
2. The authority under the Protection of Privacy Act to collect the personal information.
3. The title, business address and business telephone number of an employee who can answer questions about the collection.
4. The public body's intention, if any, at that time to input the information into an automated system to generate content or make decisions, recommendations or predictions.

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, unnecessary 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

OneCity: Data Collection Statements

Standard
Generative Artificial Intelligence

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

Program Impacted	*Project and Asset Management* The City of Edmonton's projects are well managed and assets are maintained for accountable service delivery *Technology and Data* The City of Edmonton's technology and data are leveraged to enable quality decision-making and enhance innovative service delivery.
Approved By	City Manager
Date of Approval	July 25, 2024
Approval History	Update to section 3.2. approved July 29, 2025
Next Scheduled Review	July 2026

Purpose

The purpose of this standard is to govern the use, inputs and outputs of generative artificial intelligence tools.

Application

This standard applies to any person who reports to the City Manager and provides services to the City of Edmonton under a contract of employment, contract for the provision of services, or in the capacity of student or volunteer.

Definitions

Generative artificial intelligence (AI) tools refers to products, services, libraries, models and capabilities, whether online or not, that model patterns and structures using large quantities of data in order to generate new outputs based on inputted prompts — examples include, but are not limited to: text, images, video, audio, structures, computer code, synthetic data, workflows and models of physical objects.

Sensitive information refers to any data that is classified as confidential or restricted.

Specifications

1. Compliance
   - 1.1. Use of generative AI tools must be consistent with all applicable laws (including the *Protection of Privacy Act [POPA],* the *Access to Information Act* [ATIA] and legislation relating to artificial intelligence,

copyright, human rights, data privacy, and data security, etc.), and all applicable professional regulatory requirements, as well as the City's *Code of Conduct* and *Administrative Directive A1429D: Acceptable Use of Communication Technology*

1.2. Use of generative AI tools, other than tools supported by the City of Edmonton, is prohibited regardless of the computing device, network or location. It is the responsibility of Employees to ensure that the use of any other generative AI tools for City purposes is approved in advance, following the City's technology intake process.

1.2.1. City-approved technologies that are upgraded with generative AI capabilities must also go through the City's technology intake process.

1.3. All generative AI inputs and outputs are considered City of Edmonton records and are subject to the City's record management policy tools, including the City of Edmonton's Classification and Retention Schedule.

2. Data Privacy and Confidentiality

2.1. Sensitive information must not be provided as inputs to generative AI for any purpose, including for training or testing generative AI models outside of the City's control.

2.1.1. Providing inputs to generative AI without City enterprise controls is considered the same as releasing that data to the public.

2.1.2. The Protection of Privacy Act (POPA) requires that the City inform individuals at the time of collection if their personal information will be inputted into "an automated system to generate content or make decisions, recommendations or predictions." The City of Edmonton complies with the Act and includes a collection statement with every collection of personal information from individuals.

3. Accountability, Use and Validation of Generative AI Outputs

3.1. All outputs must be reviewed by humans before being used.

3.1.1. The human reviewer is fully accountable for the accuracy and timeliness of the output.

3.1.2. The human reviewer is also responsible for ensuring that the output is inclusive, respectful and aligns with all City's guidelines.

3.1.3. The human reviewer must not use materials that breach copyright or other applicable laws and legislation.

3.1.4. When using generative AI, City staff must not misrepresent expressly or by omission the origin of generated outputs.

3.2. All generative AI outputs, including audiovisual, in City of Edmonton public (external) communications are subject to approval by the Chief Communications Officer, after receiving approval from the City Clerk (or designate) and the City Solicitor (or designate). These outputs include:

- AI-generated or AI-edited images
- AI-generated audio, including human voiceovers
- AI-generated video

4. User Resources

4.1. The *Manual of AI Processes* provides an up-to-date listing of requirements for AI use in functions that span the corporation.

Guideline
Non-personal Data

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	November 13, 2026

Guideline Statement

This guideline provides guidance on the creation of non-personal data from personal information, the acceptable use and disclosure of non-personal data and the record-keeping requirements under the *Protection of Privacy Act* (POPA) when creating non-personal data.

This guideline falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy*.

Scope

This guideline 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.

Guideline Description

This guideline provides direction on:

- the creation of non-personal data, including the required documentation,

- the assessment of non-personal data for risk of individual re-identification, and
- the protection of non-personal data.

Definitions

Aggregation is the process of grouping data, removing unnecessary details and summarizing it for analysis or reporting.

Blurring means the process of adding random noise to data values, such as age or date of birth, to reduce the risk of re-identifying individuals while keeping the data useful for analysis.

Bucketing is a form of aggregation that groups specific data values into broader categories.

Correlation criterion means the standard that must be met to ensure that individual records within a set of data (dataset) cannot be matched to other records about the same person found in separate datasets.

Data derived from personal information means data created by data matching that identifies any individual whose personal information was used in the data matching.

Hashing means a one-way process that uses a special algorithm to convert data of any size into a fixed-length string of characters, known as a hash value or digest.

Identifiers are pieces of data that are unique, or mostly unique, to an individual. Examples are name, personal telephone number and identification numbers such as Social Insurance Numbers (SIN) or Employee ID numbers.

Individualization criterion means the standard that must be met to ensure data does not allow a person to be isolated or distinguished from others within the dataset.

Inference criterion means the standard that must be met to ensure data does not allow personal information to be guessed or deduced from the data when combined with other available information.

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.

Quasi-identifiers are pieces of data that may not identify an individual on their own, but a collection of quasi-identifiers could identify an individual. Examples of quasi-identifiers include home address, age, an anecdote about a person, family affiliations or professional associations.

Scrambling (magic numbers) refers to the process of using numbers to perform basic arithmetic operations on the input data to obscure the output data

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

Non-personal data is data that is changed so that an individual cannot be identified from it. To make individuals non-identifiable, creators of non-personal data use various methods, including but not limited to scrambling, hashing, aggregation and blurring.

Under the *Protection of Privacy Act (POPA)*, the City is only permitted to create non-personal data for the purposes of:

- research and analysis, and
- planning, administering, delivering, managing, monitoring or evaluating a program or service.

Aggregation of data for the *purpose of anonymization* is considered the creation of non-personal data. The following are actions taken under the *Access to Information Act* (ATIA) and are *not* considered the creation of non-personal data:

- redacting (blocking out or removing) identifiable information from a record before disclosing it in response to a request under ATIA,
- creating a summary or new record from existing unstructured data to help an applicant get the information they asked for (duty to assist) under ATIA, and

- proactively or routinely disclosing information or records deemed to be routinely available under section 90 of ATIA that have been filtered or edited to exclude personal identifiers to allow for disclosure.

Aggregation of any data for the *purpose of producing statistics and reporting numerical trends* is also not considered to be the creation of non-personal data.

Documenting the Creation of Non-Personal Data

The *Protection of Privacy Act, SA 2024, c P-28.5, s21(4)* specifies that the creation of non-personal data must be documented as a record that includes:

- a description of the *personal information* or *data derived from personal information* used to create the non-personal data,
- the purpose for creating the non-personal data,
- the method used for creating the non-personal data, and
- an assessment that confirms the identity of the individual, who is the subject of the non-personal data, cannot be identified or re-identified from the data.

This record will support the data itself and fall under the same retention and disposition schedule as the non-personal data.

Assessing Re-identification Risk

The creation or anonymization of personal information should be assessed against the following criteria to ensure that the non-personalized data truly protects privacy:

- *Correlation criteria: t*he assessment confirms that one cannot connect an individual's existing personal information across two or more separate datasets. If one could connect, then this criterion would not be met. For example, if one has a dataset with postal codes and information A, B, C and D and a second dataset with postal codes and resident names, you may be able to learn information A, B, C and D about those individuals by connecting the two datasets.
- *Individualization criteria*: the assessment confirms that one cannot single out or distinguish an individual from others within a dataset. If an individual could be singled out, then this criterion would not be met. For example, if a dataset has a single line with sufficiently rare combinations of demographic information or other quasi-identifiers, there is a reasonable chance that the individual could be identified.
- *Inference criteria:* the assessment confirms that one cannot infer or deduce new personal information about a person from the data, when combined with other publicly available information. If one could infer or deduce, then this criterion would not be met. For example, guessing information from publicly available sources might occur if the information includes links to other sources, such as residential

addresses, which can be associated with owners/residents and reveal additional personal information about them.

Assessments are based on an assumption of reasonableness, meaning an individual with average technical skill, access and means should not be able to identify or distinguish an individual using ordinary (non-criminal) methods.

It is unnecessary to show there is zero risk of re-identification; however, the assessment results must show that the residual risks of re-identification are very low. Assessments need to consider context, including:

- the circumstances related to the anonymization of personal information, in particular, the purposes for which the public body intends to use the anonymized information,
- the nature of the information,
- the correlation, individualization and inference criteria,
- the measures required to re-identify the individual, taking into account the efforts, resources and expertise required to implement those measures.

Protecting Non-personal Data

Security Measures

Non-personal data must be protected by reasonable safeguards against risks such as unauthorized access, collection, use, disclosure or destruction. This includes classifying non-personal data in accordance with the *City of Edmonton Classification and Retention Schedule* and implementing appropriate safeguards in alignment with City of Edmonton policy tools.

If non-personal data is created by an automated system, human auditing and validation measures must be in place to ensure the data's accuracy and reliability.

Disclosure

Non-personal data may be disclosed to another public body — for example, to another municipality, a school board or the Government of Alberta — for any purpose.

The City of Edmonton will disclose non-personal data to an individual outside of the corporation only for the following purposes:

a) research and analysis, and/or
b) planning, administering, delivering, managing, monitoring or evaluating a program or service.

Disclosure may occur only after the outside individual signs an agreement that complies with the *Creation and Protection of Non-personal Data Administrative Standard.* Checking a box to agree to terms and conditions constitutes such an agreement.

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 policies, including the *Corporate Records and Information Management Accountability Model (RASCI)*. Failure to comply with this guideline 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

Corporate Records and Information Management Accountability Matrix (RASCI)

Creation and Protection of Non-personal Data Administrative Standard

Guideline
Records Management for Physical Records

Program Impacted	Strategy & Business *The City of Edmonton's corporate processes are robust and helpful for integrated service delivery.* 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	March 18, 2025
Approval History	N/A
Next Scheduled Review	March 2027

Guideline Statement

This guideline provides direction to employees on corporate records and information management, including specific guidance on how, when and why to keep, dispose or archive physical City records and information in a compliant and secure manner.

This guideline falls under the Lifecycle Management (LM) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

This guideline provides direction for all City employees, contractors and volunteers who create, receive, access or use records in any physical format, including digital records stored on physical mediums. Employee records management roles and responsibilities are outlined in the Corporate Records and Information Management Accountability Model (RASCI.)

Guideline Specification

City employees, contractors and volunteers who create, receive, access or use records in any physical format are responsible for managing them.

Although there has been a significant push to go digital in the past couple of decades, there are still times when the City needs to keep physical records for one or more of the following reasons:

- *Legislation*: Federal and provincial laws say that some types of records need to be kept in a physical format and managed that way. Example record types include election ballots and contracts that require wet-ink signatures, such as records that create or transfer interests in land.
- *Preservation:* Paper records are still the only format guaranteed to be readable for long periods of time. Some records must be kept by the City for 25 years or longer, and some need to be kept permanently without alteration; for example, Council meeting records have a permanent retention. The complete meeting file is printed on archival paper, filed and stored permanently.
- *Process-driven considerations:* Sometimes it makes business sense to keep a record in a physical format. For example, digitization isn't practical for some paper records. It might be too expensive or take too much digital storage space to scan and store oversized records like old building blueprints.

Definitions

Centralized filing system refers to the files of one or more business units stored in one location to improve management, access and control.

Certificate of destruction refers to a document confirming the secure destruction of specific records in conformity with City of Edmonton Classification and Retention Schedule. A certificate of destruction must be completed whenever official copies of the City's records are destroyed. The certificate provides information about the records that were destroyed, including but not limited to:

- certificate number
- file names or other description
- retention rules
- dates covered by the records
- destruction method

City of Edmonton Classification and Retention Schedule refers to a living policy document that categorizes records based on similar use and purpose to facilitate lifecycle management. The schedule provides rules that identify the length of time a record needs to be kept (retention period), what to do with the record when it is no longer needed (disposition method) and supplementary information.

City record refers to recorded information in any form that is acquired or developed during the course of City business.

Corporate Records Centre (CRC) refers to the off-site secure storage facility managed by the Corporate Records and Information Management team within the Office of the City Clerk that provides for the transfer, processing, storage, retrieval and secure destruction or transfer of physical City records.

Non-transitory records refers to City records and information that demonstrates the City's activities, business transactions and decisions. There are many different types of non-transitory records, each with specific rules about how long they need to be kept (retention period) and whether to destroy them or transfer them to archives (disposition). These rules are outlined in the City of Edmonton Classification and Retention Schedule.

Physical record refers to information recorded in a physical format, such as paper, microfilm, sound recordings, videotapes, x-rays, microfiche, aperture cards, or photographs. Physical mediums that contain digital City information are considered physical records. Mediums include hard drives, USB drives, disks, SD cards, magnetic tapes and audiovisual media such as CDs and DVDs.

Records lifecycle refers to the life span of a record from its creation or receipt to its final disposition. There are four stages:

1. *creation or receipt:* The initial receipt or creation of City records, including naming, drafting and formatting.
2. *access and use*: The classifying, filing, accessing and sharing of records and information.
3. *storage and maintenance:* The maintenance and storage of records for the legal and operational time period required (retention period) in the correct locations with the correct access.
4. *destruction or transfer:* The final outcome of a record's lifecycle, referred to as disposition. A record is due for disposition when it has met its retention period requirements as defined by the City of Edmonton Classification and Retention Schedule. Disposition could be the destruction of the record or a transfer of record ownership to another entity.

Transitory records refers to City records and information that may be required for a limited period of time for the completion of a routine action or the preparation of a corporate record but not required to meet statutory obligation or to sustain administrative or operational functions. Transitory records only possess an immediate value and should be disposed of thereafter.

Physical Record Types

Physical records come in many formats, some more official than others. Information can be recorded on paper, microfilm or microfiche, CDs, DVDs, videotapes, photographs, sticky notes, data tapes, hard drives and notepads, among many others. If information is written or recorded on something you can touch, it's a physical record.

Filing Requirements by Frequency of Use

Record storage requirements depend on how often a record is used; frequently used records are stored onsite, while less commonly referenced records should be stored offsite. The most cost-effective storage location for most physical records is at the City's offsite corporate records storage facility, the Corporate Records Centre (CRC), where the City is also able to manage the full lifecycle of the records correctly — see Table 1. Records stored offsite can be delivered to the business area location upon request.

Table 1: City Records and Information - Frequency of Use and Recommended Storage Location

Term	Frequency of Use	Storage Location
Active	used on a regular basis	stored onsite so records are easily accessible to the appropriate user(s)
Semi-active	used occasionally but are not required for immediate access	stored at the Corporate Records Centre until records have reached the end of their retention period
Inactive	no longer accessed or used to conduct current business	stored at the Corporate Records Centre until records have reached the end of their retention period

Filing Requirements by Security Classification

Physical records with different security classifications have different filing requirements (see Table 3). Security classifications provide a way to organize data and information so that they are available only to the right people in the right roles. All City records and information must be assigned a security classification, as per the City of Edmonton Classification and Retention Schedule.

Table 3: Physical Filing Requirements by Security Classification

Security Classification	Filing Requirements
Public	Physical public documents with current information may be stored in the most convenient location. Out-of-date transitory documents should be placed in a grey shred bin.

Security Classification	Filing Requirements
Internal	Files are stored in a location that is accessible to City employees but not accessible to the general public, such as a shelving unit in a staff-only area.
Confidential	Files are stored in a locked file cabinet or room when not in use.
Restricted	Files are stored in a locked file cabinet or room when not in use. The only keyholders are those who also have permission to access those documents.

Filing Requirements by Transitory/Non-transitory Classification

Physical records, like digital records, are primarily classified as either transitory or non-transitory. Transitory records are temporary informal records. Employees need transitory information for only a short period of time, often for reference. Transitory records may help employees to complete routine actions or prepare non-transitory records. They do not need to be kept for legal reasons or to support ongoing work. Transitory physical records can include rough notes, copies, drafts, working materials and reference materials.

Non-transitory records record activities, transactions and decisions made by City employees; they contain information that needs to be kept and managed. Non-transitory record types need to be kept for a set period of time for legal reasons or to support ongoing work. Non-transitory records can include receipts, permits, licenses, applications and completed forms.

Non-transitory Active Records

If non-transitory records are in regular use, they are considered active records and are kept onsite. Each business area that creates or receives physical records should have an area where they can securely store records in a central location, using a standardized business area filing system. Examples of different types of filing systems are listed in Table 2.

Table 2: Physical Record Filing Systems

Physical Record Filing Systems	
Alphabetic	Records are named using full words or individual letters. Names may include project names or geographic locations. Records are sorted, shelved or boxed in alphabetical order to be retrieved easily.
Alphanumeric	Records are named using a combination of letters and numbers. Names may include company name, subject or geographic location, as well as date or chronological number. Records are sorted, shelved or boxed in alphabetical order or ascending numeric value for retrieval, depending on whether the record name begins with a number or a letter.

Physical Record Filing Systems	
Functional	Records are classified based on the high-level work functions such as human resources or financial management. A second and third level of classification may also be used, with the second level representing activities carried out under each function, and the third level representing the types of records or transactions (records series) that are generated as part of each activity.
Numeric	Records arranged by number. The number can be part of the record itself, such as an invoice number, or it can be assigned, like a file number.
Subject	Records classified by specific subject matter and arranged in alphabetical order by subject. This is the system usually found in libraries, with subject titles such as Psychology or Woodworking.

Non-transitory Semi-active and Inactive Records

The City's physical records are stored offsite at the Corporate Records Centre (CRC) once they are no longer actively being used. Business areas work with their Department Records Advisors (DRAs) to prepare an inventory, box records for pick up and transfer semi-active and inactive physical records to the CRC. Once CRC staff receive a records transfer request, they pick up the boxes. The inventory is entered into a records management software application that manages the lifecycle, storage location and requests associated with physical records. City departments can request delivery of their semi-active and inactive records when needed and must return them when they are no longer regularly in use.

Non-transitory Record Disposition

Disposition is the action taken after City records and information have reached the end of their retention period, a length of time the City needs to retain records based on business, legal, and historical requirements. The retention period for each record series is identified in the City of Edmonton Classification and Retention Schedule. Disposition is the last stage of a record's lifecycle.

City records and information in the custody and control of City staff, contractors and volunteers must be disposed of defensibly once they have been kept for the required time. Arbitrary and unplanned records destruction is considered to be suspicious activity, especially if the information is needed for an information request or litigation. Records destruction can be found by courts to be illegal destruction of evidence, which may bring serious legal sanctions against the organization, including court fines.

To avoid these consequences, the City has developed and implemented a program that will ensure compliance with legislation and operational needs while providing a secure and safe method for the disposition of records and information.

Disposition Roles and Responsibilities

Records management roles and responsibilities are listed in the *Corporate Records and Information Accountability Model (RASCI).* The City Clerk or delegate must authorize all records dispositions, and only the Corporate Records Centre is allowed to destroy non-transitory physical records.

Methods of Disposition

Each record series in the City of Edmonton Classification and Retention Schedule is assigned a disposition outcome: destruction, archives or permanent. On rare occasions, the City will also transfer ownership of City records to another entity, such as when Drainage Operations moved to Epcor.

Destruction

Records must be destroyed using a method appropriate for their medium and content. Sensitive or confidential information must be rendered unreadable. The method used for records destruction must also be cost-effective and environmentally friendly.

The Corporate Records Centre is responsible for destroying physical records, as well as physical mediums that store digital records.

Methods of destruction:

Paper records are shredded to a high-security particle size, compliant with the DIN 66399 P-3 standard, by a NAID AAA-certified vendor. Shredding is conducted under surveillance at the Corporate Records Centre. Shredded material may be recycled or pulped.

In most cases, sanitization is recommended to remove sensitive information from physical devices storing digital records. Methods include:

- Destroying the medium by shredding, pulverizing and incinerating when the storage device is no longer required by the business area. Destruction is conducted on-site at the Corporate Records Centre using an authorized contracted shredding services.
- Purging accomplished via degaussing or secure erasing of a hard drive. Degaussing magnetically erases digital information from tape devices and hard drives but is not effective in clearing data from DVDs and CDs.

Archives

Records and information are transferred to the City of Edmonton Archives when the primary corporate value has expired but the record maintains historical value, as identified in the City of Edmonton Classification and Retention Schedule. Custody is transferred through the physical transfer of records and a certificate of transfer from the CRC.

Although these records are now in the custody and control of the City of Edmonton Archives, they may still be accessed by City staff as required, either by viewing onsite at the City Archives or reproduced in an appropriate format. The City of Edmonton Archives may choose to preserve the entire transferred collection or retain a sample selection.

Permanent

Permanent records must be retained indefinitely at the CRC. Continued preservation is required to comply with legislation or to support ongoing City operational requirements. Examples of permanent records are the Corporate General Ledger, as required by the Income Tax Regulation, and Building and Development Permits, as required for operations to immediately issue compliance certificates.

Transfer to Another Entity

Records may need to be transferred to a third-party entity if the City transfers ownership of a program or service to another provider. Transfers still must undergo the proper disposition process, resulting in the required appropriate documentation. For example, before drainage records were transferred to EPCOR, they received sign off by the appropriate delegated authority.

Calculating Disposition

Disposition is identified using the following formula:

Date of Retention Trigger + Length of Retention Period = Disposition Date

Find the retention trigger and retention period in the *City of Edmonton Classification and Retention Schedule*.

Example:

Date of Document:	July 15, 2010
Retention Trigger:	Current year (end of year) = Dec 31, 2010
Retention Period:	2 years

Retention Trigger	+	*Retention Period*	=	*Disposition Date*
December 31, 2010	+	2 years	=	December 31, 2012

Suspending Disposition

Records and information on hold need to have disposition suspended, even if they have reached their disposition date. The Department Records Advisor will determine if any of the listed records on a Notice of Disposition has an associated hold. See Table 4 for types of holds.

Table 4: Types of Holds

Type of Hold	Definition
Legal	Legal holds suspend disposition of records related to current or pending litigation. Legal Services or the Corporate Records and Information Management team within the Office of the City Clerk contacts business areas and DRAs to advise them of legal holds.
Information request	Information request holds suspend disposition of information requested under the provincial protection of privacy and access to information acts.
Audit	Audit holds suspend disposition of information relating to a current or pending audit. Corporate Records will contact DRAs to advise them of audits.
Schedule revision	Schedule revision holds suspend disposition for records included in records series that are under review.

Notice of Disposition

A Notice of Disposition must be prepared and retained when City records and information are destroyed. This provides documentation proving compliance with legislation and with the City of Edmonton Classification and Retention Schedule. Branch Managers or delegate are responsible for signing off that the business area's record advisor has no concerns with the records disposition; the City Clerk or delegate signs to authorize the disposition.

A Notice of Disposition provides information about the records that were destroyed, including:

- record filing names
- retention rules and information
- record date range
- dates the records were approved to be destroyed
- destruction method

A Notice of Disposition becomes a Certificate of Destruction once all parties have reviewed and signed the notice and the destruction or transfer of records has been completed.

Copies of the Notice of Disposition and Certificate of Destruction will be processed as follows:

1. The Certificate Number is applied to the Notice of Disposition by CRC staff.

2. The records are updated as destroyed in the records management software and the certificate number added.
3. A paper copy of the Notice of Disposition and the corresponding Records Transfer are filed at CRC.
4. The completed Certificate of Destruction is shared with the DRA.

A Notice of Disposition and Certificate of Destruction prove compliance with legislation and with the City of Edmonton Classification and Retention Schedule. Certificates of Destruction may be referred to and must be produced as evidence when requested by a court of law.

Transitory Record Disposition

A transitory record is a City record that may be required for a limited period of time for the completion of a routine action or preparation of a corporate record, but is not required to meet statutory obligations or to sustain administrative or operational functions. Examples of transitory records include:

- copies
- drafts
- working materials
- informal to-do lists and reminders

Temporary Use

Transitory records have no further value or usefulness beyond an immediate or short-term use. They should not be retained after that time. City employees are responsible for the routine destruction of transitory records.

Secure Shredding

City transitory records must be collected via secure grey shred bins. Transitory records may contain sensitive, confidential or personal information. They are a liability to the City of Edmonton and must be disposed of in a secure manner. Employees are responsible for using the grey bins for transitory records. Corporate Records Centre staff are responsible for secure destruction of these records.

Bins should be located in a convenient area within the business unit for all staff to use and be readily accessible for removal and replacement by Corporate Records Centre staff. Bins should not be moved from this location without notifying the Department Records Advisor or Key Coordinator.

If locked bins are not available, employees may place transitory City records to be shredded in boxes labelled *Security Shred - CRC* and store them in a locked room. When a business area has filled four or five boxes, an employee should call the CRC for pick-up.

When a grey bin is 80% full, an employee can request that a bin be picked up; CRC staff will replace the bin within a week. Pick up requests must include the location and number of bins and should be directed to the Corporate Records Centre. See OneCity for contact information.

References and Supporting Resources

Administrative Policy A1477: Data and Information Management

City of Edmonton Classification and Retention Schedule

Corporate Information Management Glossary of Terms

Corporate Records and Information Management Accountability Model (RASCI)

Standard

Release of Personal Information to Other Public Bodies

This standard 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	June 3, 2026
Approval History	N/A
Next Scheduled Review	June 3, 2027

Standard Statement

This standard governs the disclosure of personal information to other public bodies and federal institutions, including municipal, provincial and federal law enforcement agencies, under the *Protection of Privacy Act (POPA)* s 13(1).

This standard falls under the Privacy (P) functional domain, as defined in *A1477 Data and Information Management Administrative Policy.*

Scope

This standard applies 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

Law enforcement, as defined in ATIA, means:

a) policing, including criminal intelligence operations,
b) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or
c) proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred.

Law enforcement agencies include, but are not limited to, Alberta Justice, RCMP, provincial, municipal and First Nations' police services and the Canada Customs and Revenue Agency (CCRA).

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.

Public body, for the purposes of this standard, includes any of the following entities:

- Any government institution, including departments, agencies, boards, commissions, or Crown Corporations of the Government of Canada or as defined in the Canada *Access to Information Act, R.S.C., 1985, c.A-1*.
- Any department, branch, or office of the Government of Alberta or other province.
- The Legislative Assembly Office and any independent offices of the Legislature.
- Any agency, board, commission, corporation, or other body designated as a public body within applicable regulations.

- Any local public body, such school boards, post-secondary institutions, public health care institutions, municipal governments and the boards, committees, commissions, panels, agencies or corporations created or owned by them, or as defined in the *Access to Information Act* (ATIA) - see below.

For the full legal definitions, see the Access to Information Act, Section 1 and the Protection of Privacy Act, Section 1.

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.

Standard Specification

Responsibilities

The City Manager or delegate shall:

a. approve this standard and amendments.

The Department Contact Person shall:

a. liaise with representatives of public bodies when requests for personal information are made, and
b. ensure records related to the disclosure are maintained in accordance with the City of Edmonton Classification and Retention Schedule.

Disclosure Requirements - Disclosure Enabled or Required by an Enactment of Alberta or Canada

Requests to the City of Edmonton from a public body or a federal institution for personal information in accordance with an enactment of Alberta or Canada must:

- be in writing, and
- be referred to an appropriate department contact person.

The request must contain the following information:

- the name of the individual whose information is requested;
- the exact nature of the information desired;
- the receiving public body or federal institution’s collection authority or authorities, including specific sections of Acts or Regulations that authorized collection;
- the purpose for which the public body will use the information;
- the public body or federal institution's file number; and
- the name, title and address of the person authorized to make the request.

Disclosure Requirements - Law Enforcement Agency

Requests to the City of Edmonton from a law enforcement agency must be:

- in writing using the Law Enforcement Disclosure form or a site-specific form that includes all the same elements, and
- referred to an appropriate department contact person.

The City of Edmonton will not disclose personal information to a law enforcement agency under section 13(1)(p) unless the agency can provide sufficient information to satisfy that the purpose relates to a bona fide law enforcement matter as defined in POPA. Personal information will not be disclosed merely based on suspicion, surmise or guess.

The Law Enforcement Disclosure form, which demonstrates an authority to disclose personal information under section 13(1)(p), must be completed, containing the following information:

- the name of the individual whose information is requested;
- the exact nature of the information desired;
- the authority for the investigation;
- the purpose for which the requesting law enforcement agency will use the information;
- the law enforcement agency's file number; and
- the name, title and address of the person authorized to make the request.

The department contact person will:

- review the form to confirm completeness;
- consent to or refuse the disclosure of personal information;
- ensure that only the information necessary to answer the request is disclosed if the request is granted;
- consult with the Corporate Access and Privacy in the Office of the City Clerk if unsure there is an authority for the disclosure of personal information;
- ensure that when the record is provided, appropriate safeguards are used (for example, encryption); and
- ensure that a record of when and to whom personal information was released is kept in a separate file. This record must be retained in accordance with the City of Edmonton Classification and Retention Schedule.

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 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 policies, 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, legal risk, information breaches and complaints from the public.

References and Supporting Resources

Legislation

- *Access to Information Act, SA 2024, c A-1.4*
- *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
- Law Enforcement Disclosure Form
- Corporate Information Management Glossary of Terms
- Corporate Records and Information Management Accountability Matrix (RASCI)