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)