



CITY PROCEDURE

Privacy Incident Response and Notification

Procedure Title	Privacy Incident Response and Notification		
Procedure Number	507-6	Approved Date	2026-07-16
Department	Legislative and Legal Services	Last Amended	
City Manager Signature	"S. Bourke" (signed)	Last Reviewed	
		Signature Date	2026-10-09

1. Purpose

- 1.1. The purpose of this procedure is to establish processes for identifying, containing, assessing, reporting, and preventing Privacy Incidents in accordance with Provincial Privacy Legislation and City policy.

2. Scope

- 2.1. This procedure applies to all Employees.

3. Definitions

The definitions in [Policy 507 Privacy Management](#) apply to this procedure. In addition, in this procedure:

- 3.1. **"GIS and ITS"** means the City's GIS and ITS Department, responsible for maintaining and safeguarding the City's information technology systems.
- 3.2. **"Department Head"** means the senior Employee in the highest level of authority of a department.
- 3.3. **"Legal Services"** means a legal counsel appointed to act on behalf of the City, or their designate.
- 3.4. **"Privacy Coordinator"** means the position responsible for operational administration, carrying out the powers, duties and functions related to Provincial Privacy Legislation that are delegated to the Privacy Coordinator by the City Manager.
- 3.5. **"Real Risk of Significant Harm" (RROSH)** means that a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of Personal Information (or data derived from Personal Information).
- 3.6. **"Supervisor"** means the person in the City who is immediately responsible for or in charge of the Employee.



CITY PROCEDURE

Privacy Incident Response and Notification

4. Procedure & Guidelines

4.1. Identification and Containment

- 4.1.1.** An Employee who suspects or confirms that a Privacy Incident has occurred must immediately take reasonable steps within their ability to contain it (see Schedule A for examples), including:
 - a.** Securing affected systems, records or devices;
 - b.** Disabling unauthorized access; and
 - c.** Recovering or limiting further disclosure of information, where possible.
- 4.1.2.** Containment must not delay reporting under section 4.2.
- 4.1.3.** The Employee must document known details of the Privacy Incident, including time, location and nature of the information involved.
- 4.1.4.** Employees must not destroy or alter information that may be required for investigation.

4.2. Reporting

- 4.2.1.** Employees must report any suspected or confirmed Privacy Incident to their Supervisor and the Privacy Coordinator without unreasonable delay.
- 4.2.2.** Where a Privacy Incident involves City systems, devices or accounts, the Privacy Coordinator or the reporting Employee must also notify GIS and ITS immediately so that technical containment can begin. If theft or other criminal activity is suspected, the Employee must notify their Supervisor, and the Supervisor must contact law enforcement; in an emergency, any Employee may contact law enforcement directly.
- 4.2.3.** The Privacy Coordinator must receive and manage privacy complaints from members of the public regarding the collection, use or disclosure of Personal Information.
- 4.2.4.** Complaints may be submitted in writing or through another method permitted by the Privacy Coordinator, must be acknowledged promptly, and must be responded to within 30 business days.
- 4.2.5.** Where the City's response does not resolve the complaint, or the City does not respond within 30 business days, the Privacy Coordinator must advise the individual of the right to complain to the Information and Privacy Commissioner within 60 business days.

4.3. Investigation and Risk Assessment

- 4.3.1.** Every Privacy Incident must be escalated to the Privacy Officer. The Privacy Coordinator, under the direction of the Privacy Officer, will:
 - a.** Lead the investigation of the Privacy Incident.
 - b.** Gather and review relevant information regarding the Privacy Incident;



CITY PROCEDURE

Privacy Incident Response and Notification

- c. Consult with affected departments;
- d. Determine the nature, scope and cause of the Privacy Incident; and
- e. Prepare an investigation record stating the nature, scope and cause of the Privacy Incident, the containment and mitigation steps taken, and the steps identified to prevent recurrence.

4.3.2. The Privacy Officer must:

- a. Determine whether the Privacy Incident meets the RROSH threshold, in accordance with section 4 of the Protection of Privacy (Ministerial) Regulation, and may obtain advice from Legal Services; and
- b. Document the RROSH determination and the reasons for it.

4.4. Notification

4.4.1. Where the Privacy Officer determines that RROSH exists, the Privacy Officer must give notice, without unreasonable delay, to:

- a. Affected individual(s);
- b. The Office of the Information and Privacy Commissioner of Alberta; and
- c. The Minister responsible for POPIA (the Minister of Technology and Innovation).

4.4.2. Each notice must be given in writing by a method authorized under section 53 of POPIA and must contain the information prescribed by sections 4(3) to 4(5) of the Protection of Privacy (Ministerial) Regulation.

4.4.3. Where RROSH is not met, the Privacy Coordinator will determine whether notification to individuals is nonetheless appropriate and will document the rationale for any decision not to notify.

4.5. Mitigation

4.5.1. The Privacy Officer (or, for a Privacy Incident that does not meet the RROSH threshold, the Privacy Coordinator) determines the mitigation measures required to reduce a risk of harm, and the responsible Department Head (or, where more than one department is involved, the Department Heads jointly, as coordinated by the Privacy Coordinator) must implement them. Measures may include:

- a. Account monitoring or resets;
- b. Access restrictions;
- c. Credit monitoring, where appropriate; and
- d. Additional safeguards or controls.



CITY PROCEDURE

Privacy Incident Response and Notification

4.6. Documentation

- 4.6.1. The Privacy Coordinator will maintain a register of all Privacy Incidents, including:
- a. Incident details;
 - b. RROSH determinations;
 - c. Notification decisions; and
 - d. Mitigation actions taken and the results of any post-incident review.

4.7. Prevention and Continuous Improvement

- 4.7.1. For a Privacy Incident that meets the RROSH threshold, or where the Privacy Officer otherwise considers it warranted, the Privacy Officer must lead a post-incident review to identify root causes, with support from the responsible department and, as needed, other subject matter experts. For other Privacy Incidents, the Privacy Coordinator shall keep a Record of lessons learned.
- 4.7.2. The responsible Department Head must implement the corrective actions identified by the review, in coordination with the Privacy Officer, which may include
- a. Updates to departmental practices or standard operating procedures;
 - b. Enhancements to safeguards; and
 - c. Training and awareness initiatives.
- 4.7.3. The Privacy Officer must monitor Privacy Incidents for recurring issues and systemic risks and recommend improvements to safeguards and procedures.

5. Roles and Responsibilities

- 5.1. The City Manager will review and approve this procedure and any amendments.
- 5.2. Employees will comply with this procedure.

6. Attachments

- 6.1. **Schedule A:** Examples of Common Privacy Incidents and Potential Containment Actions.

7. Version History

Action	Date	Description
New Procedure	2026-07-16	

CITY PROCEDURE

Privacy Incident Response and Notification

Schedule "A": Examples of Common Privacy Incidents and Potential Containment Actions.

Potential Incident	Potential Containment Action
Misdirected email to wrong client, Employee or other unintended recipient.	- Request an email recall through your email system, if the function is available. - Where a group email includes an unintended recipient remove the unintended recipient, resend email requesting staff to delete and not respond to the original email. - Contact the unintended recipient, advising information was sent in error and request them to delete the email from both their inbox and then the deleted folder. Confirm information was not read and no copies were made.
Documents are mailed or sent to the wrong individual.	Contact unintended recipient and request the records be returned or destroyed.
An Employee uploads documents for one client into another client's file.	- Restrict access or delete the document from the file. - Review to ensure correct Personal Information is in the right file. - Contact the unintended recipient and request them to delete it on their side (if possible). - Confirm no copies of the information were made or retained.
An Employee's work laptop and/or cellphone is stolen.	- Contact GIS and ITS to request device be remotely wiped, if possible, and request them to confirm if any attempts at log-in were received after last known Employee's use. - Contact law enforcement to report theft.
An Employee accessed third party personal information (such as family members, friends, neighbors etc.) on the City's database or file system.	Restrict access to the files.
Potential inadvertent destruction of Personal Information records before their retention period has been met.	- Confirm and investigate missing records. - Determine if the missing records had met their retention timeframes and were properly destroyed or if they were inadvertently destroyed. - If the records were digital, contact GIS and ITS to determine if they can be recovered from backups.

Note: Following the above containment actions does not absolve the Employees responsibility to report the Privacy Incident to their Supervisor and the Privacy Coordinator.