Privacy Breach Protocol

Guideline No.: CIMS-P003
Version No.: No. 2.0
Issued On: March 18, 2025
Approval date: February 27, 2025
Issued By: Corporate Information Management Services, City Clerk's Office
Subject: Privacy Breach
Keywords: Breach, Incident, Privacy, Privacy Investigation, Privacy Analysis

Foreword: City of Toronto Information Management Policies and Standards are the official publication on the policies, standards, directives, guidelines, position papers and preferred practices given oversight under delegated authority of Toronto Municipal Code, Chapter 217, Records, Corporate (City). These publications support the City's responsibilities for coordinating standardization of Information Management in the City of Toronto.

Acknowledgements: This Guideline acknowledges the efforts, subject matter expertise, and oversight provided by the following:

- **Project Sponsor:** Kristie Pratt Deputy City Clerk, Corporate Information Management Services
- **Divisions & Business Units:** Office of the Chief Information Security Officer, Technology Services Division, Privacy Unit, Corporate Information Management Services and Records Services, Corporate Information Management Services.

Contact Information:

Kristie Pratt
Deputy City Clerk
Corporate Information Management Services, City Clerk's Office
City Hall, 13th floor, West Tower
100 Queen Street West
Toronto ON M5H 2N2
Tel: (416) 392-9683
Kristie.Pratt@toronto.ca

Table of Contents

Introduction

City of Toronto staff collect, manage, and steward a significant amount of personal information about the people who live, work, and access services in Toronto. The City's *Protection of Privacy Policy* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* establish rules and guidance that City staff must follow to ensure the protection of personal information. The City of Toronto continuously works to earn public trust and confidence as well as ensure MFIPPA compliance by implementing privacy training, tactics, and requirements that mitigate privacy risks and ensure information is properly managed.

The City recognizes that privacy breaches do occur and strives to be prepared for immediate and well-planned responses to privacy breaches by implementing a *Privacy Breach Protocol*.

This Protocol's main goal is to frame the City's approach to managing all types of privacy breaches in a clear and concise manner and ensure staff understand the required steps and their obligations should a privacy breach occur.

Corporate Information Management Services (CIMS) has a dedicated Privacy Unit responsible for establishing rules and procedures for managing privacy breaches, investigations, audits, consultations, and other privacy matters.

The Office of the Chief Information Security Officer's (OC) Cyber Incident Response Plan complements this protocol. The Cyber Incident Response Plan describes the overall strategy for responding to cyber security incidents that take place within the City of Toronto.

Purpose

The purpose of this Protocol is to provide an overview of the information management responsibilities and key actions for City staff when identifying, containing, reporting and managing a privacy breach.

Specifically, the Protocol provides guidance to City of Toronto staff, vendors, contractors, and volunteers on what steps to take when a breach of personal information occurs or is suspected to have occurred.

The objectives of this Protocol are to:

- Clearly outline responsibilities and required actions when identifying a privacy breach;

- Establish investigation and reporting processes for privacy breaches; and
- Ensure compliance with privacy legislation and related City policies.

Application

This Protocol applies to all City of Toronto Divisions, employees, volunteers, and third parties engaged by the City of Toronto.

This Protocol does not apply to breaches involving personal health information. These incidents fall under the authority of Health Information Custodians (HICs) as defined by the Personal Health Information Protection Act, including the City divisions of Toronto Public Health, Seniors Services and Long-Term Care, Occupational Health & Safety (People & Equity), and Toronto Paramedic Services. Breaches (or suspected breaches) of personal health information must be reported to Divisional privacy staff within HIC divisions.

What is a Privacy Breach?

A privacy breach occurs when personal information is improperly created, collected, used, disclosed, shared, managed, retained and / or destroyed. A privacy breach also occurs when personal information is not adequately secured and is lost or stolen.

MFIPPA defines personal information as recorded information about an identifiable individual and can include information such as names, birthdates, social insurance numbers (SIN), or client information. For a more fulsome definition of personal information please consult the City's Protection of Privacy Policy (section 2.0).

A privacy breach may occur on City premises or off-site and may be the result of inadvertent errors or willful actions by employees, third parties, partners in information-sharing agreements, or intruders. Privacy breaches can be of any size and any format (electronic or hardcopy) and they all have consequences for the City and the individuals involved.

The manner in which privacy breaches occur can vary. Common types of breaches include the unauthorized disclosure of personal information; the over-collection of data and unauthorised use of that data (for example, using water bills to determine home vacancy); lost or misplaced files; lost or stolen laptops; unauthorized access to personal information in electronic or hardcopy format (for example, a City employee or vendor is given access to the wrong files within an application); or the inadvertent disclosure of personal information (for example, human error in addressing an e-mail).

Protocol: Managing a Privacy Breach

Step 1: Prepare

Thorough preparation can prevent privacy breaches or minimize their impacts by ensuring staff are trained and prepared to take immediate and effective action when a breach occurs or is suspected to have occurred. Any Division or Unit that manages personal information should:

- Designate a point of contact within their Division or Unit for privacy-related matters, including aiding and liaising with CIMS when a privacy breach occurs or is suspected.
- Ensure all required staff complete privacy awareness training, to understand their responsibilities for appropriately handling personal information and protecting privacy when executing their operational duties.
- Restrict access to personal information to those individuals who require it to perform their duties.
- Create and document processes that ensure personal information is collected, used, disclosed, and disposed of in accordance with relevant legislation and associated regulations, standards, and other City policies.
- Ensure City staff, external vendors, and contractors review and understand the privacy responsibilities outlined in various City policies, including:
    - Privacy Breach Protocol
    - Protection of Privacy Policy
    - Privacy Impact Assessment Policy
    - Information Protection Classification Standard
    - City's Acceptable Use of Information Technology Assets Policy
    - City's Video Surveillance Policy.
- Require City staff, external vendors, and contractors to maintain a level of privacy awareness appropriate for their responsibilities.
- Complete Privacy Impact Assessments for any new or updated technologies, programs, or services that collect and/or manage personal information.

Step 2: Detect, Analyze and Report

The detection of a privacy breach may occur from a wide range of internal and external sources. Breaches can be detected by people (e.g. Divisional staff noticing an issue; through a call from the IT ServiceDesk; a member of the public through an anonymous email; or business partner or client) and through technological investigations, where the City's cyber incident response management team determines that a system containing personal information was accessed by an unauthorized party. Breaches are also detected through alert calls from third-party security service providers hired by the City.

No matter the source, once a breach or a potential breach is detected, ensure appropriate staff within the City are immediately notified of the breach, including CIMS' Privacy Unit (privacy@toronto.ca). Additionally, the Office of the Chief Information Security Officer (OC) must be contacted, if not already aware of the breach. The OC will assign appropriate staff to investigate the incident.

Step 3: Contain and Eradicate
This stage involves the development of a tailored and tactical strategy to identify the scope of the breach and prevent it from spreading. It is important to note that a containment strategy depends heavily on the type of breach and will vary for each incident. The eradication part of this stage ensures the observed threat has been removed.

Cyber security-related containment and eradication actions are services managed and facilitated by the OC. For more information, please review the OC's Cyber Incident Response Plan.

Non-cyber security-related containment (namely, physical breaches) and eradication actions are incident specific and may be services managed by the Division or Corporate Security depending on the location, severity and scale.

Containment and eradication may occur in parallel with the following steps.

Step 4: Investigate and Document
Once a potential breach is identified and containment activities are initiated, the City's Privacy Unit will assess the potential breach and determine whether a privacy breach occurred and whether a full *Privacy Breach Investigation report* is required.
The following are key privacy investigation steps and requirements:

Investigation Questionnaire
Divisional staff will be asked to complete and submit a Privacy Breach *Investigation Questionnaire* to the Privacy Unit (privacy@toronto.ca). This form will aid in determining if a breach occurred, the extent of the breach and the City's response.

Initial Privacy Assessment
Once the investigation questionnaire is submitted, the Privacy Unit will conduct a preliminary assessment which will confirm whether sufficient information about the potential privacy breach has been provided to the Privacy Unit, evaluate the nature of the personal information at issue, determine the impact of the incident, and identify the cause. The preliminary assessment will then determine whether:

- a Privacy Breach occurred;

- a full Privacy Breach Investigation Report is required;
- affected parties must be contacted; and / or
- the Information Privacy Commissioner of Ontario (IPC) must be notified.

The Privacy Unit will notify the Division in writing as to whether or not a breach occurred and if the breach warrants an Investigation. Where the Privacy Unit determines a breach did not occur or an Investigation is not required, the Privacy Unit will provide written confirmation and may include recommendations in response to the incident.

Privacy Breach Investigation

If a Privacy Breach Investigation Report is required, the Privacy Unit, with the impacted Division's support, will lead the development of the Report which will document, at minimum:

- the circumstances that gave rise to the breach;
- an inventory of personal information that was affected;
- the institutional sector or third party, if any, that had a direct or indirect role in handling the personal information involved in the breach;
- the risk of harm to the individuals affected and to the institution; and
- mitigation recommendations to prevent recurrence.

Throughout the investigation process, Divisional staff must be prepared to support the Privacy Unit in gathering data and information about the breach and documenting all response actions taken.

Step 5: Notify Affected Parties (where applicable)

The Privacy Unit, in collaboration with the Division, and Legal Services when appropriate, will consider whether to provide notice to affected individuals when a privacy breach occurs. A notice may include:

- a general description of the incident, including date(s) of occurrence;
- the source of the breach (whether it is a City of Toronto employee, a contracted party or a party to a sharing agreement);
- a list of the personal information elements relating to the individual(s) that are thought to have been, or potentially have been, compromised;
- a description of the measures taken or to be taken to retrieve the personal information, to contain the breach, and to prevent a reoccurrence;
- the name and contact information of an appropriate Divisional staff member with whom affected individuals can discuss the matter further or obtain assistance;
- if applicable, a reference to any other actions or notifications the Division has initiated or completed;
- if applicable, a commitment to inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved; and
- where appropriate, any risk mitigation plan that will be implemented by the City.

The Division, in collaboration with the Privacy Unit, will draft and issue the notice to affected parties.

When issuing notices to affected parties, it is important to consider the impact of the notification on those affected individuals. Divisions may not issue notifications in some cases to avoid potential harm. For example. notification may not be required if a breach was immediately contained, and the division confirmed there was no exposure of personal information and no resulting privacy risk to the individual.

In cases where affected parties are notified, individuals may be offered additional protections where appropriate, such as credit monitoring in circumstances that may involve the wrongful disclosure of financial information, or in scenarios that may result in identity theft.

Step 6: Notify Information and Privacy Commissioner (where applicable)
The Information and Privacy Commission (IPC) of Ontario oversees compliance with Ontario's access and privacy legislation. The IPC has a mandate to investigate privacy complaints related to personal information governed by the Municipal Freedom of Information and Protection of Privacy Acy (MFIPPA). The IPC may investigate a City privacy breach if it receives a complaint regarding the breach.

The City may also self-report privacy breaches and incidents to the IPC (although privacy legislation does not require institutions to report privacy breaches to the IPC, it is best practice for institutions to self-report substantial breaches to the IPC).

The Privacy Unit, in collaboration with the Division and Legal Services, will consider whether to notify the IPC of the privacy breach and request comment on proposed privacy protection measures. This action will be considered if the breach:

- involves sensitive personal data such as financial or medical information, or personal identifiers such as the SIN;
- can result in identity theft or some other related fraud;
- may result in physical harm; or
- can otherwise cause harm or embarrassment which would have detrimental effects on the individual's career, reputation, financial position, safety, health or well-being.

The Privacy Unit, in collaboration with the Division and Legal Services, will draft and issue the notification to the IPC as soon as reasonably possible. The notification is to include information on the nature and extent of the breach, the type of personal information involved, the parties involved, anticipated risks, steps taken or to be taken to notify individuals, and any remedial action taken. The IPC will be asked to comment on the sufficiency of the remedial actions taken and any additional actions it may recommend to the City.

If the IPC chooses to comment and requests a report back on any actions taken in relation to its comments, the Privacy Unit, Division, and Legal Services will collaborate to respond.

Step 7: Mitigate and Prevent

Mitigation

The Privacy Unit will outline breach-related mitigation recommendations either within a Privacy Breach Investigation Report or, when a full Report is not required, through written communication. When provided with mitigation recommendations, the Division shall:

- Consult the Privacy Unit to validate proposed privacy risk mitigation and harm reduction actions and tactics;
- Consider any additional or alternative privacy risk mitigation actions and tactics the Privacy Unit may propose;
- Confirm preparedness to implement proposed privacy risk mitigation actions and tactics or propose alternatives that will satisfy its privacy protection obligations;
- Where appropriate, develop a risk management plan or mitigation plan which details how risks identified during the investigation will be mitigated;
- Document the implementation of each risk mitigation action;
- Ensure recommendations outlined in the Privacy Breach Investigation Report and corresponding mitigation plan are implemented; and
- Ensure documentation of privacy risk mitigation is maintained to a standard of audit readiness.

Prevention

Additionally, where appropriate, the Privacy Unit will provide consultative support to the impacted Division to identify measures required to prevent recurrence of a similar Privacy Breach. Specifically, the Privacy Unit will:

- Review applicable Divisional policies, procedures and practices for the management of Personal Information;
- Identify possible gaps in Divisional or unit privacy protection approaches;
- Undertake training related to security and privacy, as applicable; and
- Ensure relevant staff and stakeholders are properly trained to implement any new safeguards related to the Privacy Breach.

Step 8: Log and Retain Records

The Privacy Unit shall maintain a log of all privacy breaches, as well as any recommendations resulting from investigations of these incidents and breaches. The log will be used to assist in the provision of reports to the City Clerk as well as applicable City senior leadership on the number and nature of Privacy Breaches,

All documentation related to identification, containment, investigation, remediation, communication and/or notification of a privacy breach is maintained as a CIMS' Privacy Investigation File and shall be securely retained by CIMS in accordance with the City's Records Retention By-law (retention code G0265).

References

- City of Toronto. Municipal Code Chapter 217, Records, Corporate (City) (2023)
- City of Toronto. Information Management Accountability Policy (2023)
- City of Toronto. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) (2023)
- City of Toronto. Protection of Privacy Policy (2019)
- City of Toronto. Cyber Incident Response Plan (2023)

Protocol Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective February 27, 2025.

Protocol Review

The City Clerk's Office will review this protocol and its effectiveness at the two-year mark from the effective date of this protocol, or earlier if warranted.

Appendix

Appendix A: Definitions

Collection: To gather, acquire, receive, or obtain Personal Information from or about the individual to whom the information relates, by any means and from any source.

Containment: A process or a series of activities to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of information.

Cyber Incident: An occurrence that actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Disclosure: To release or make available Personal Information by any method (e.g., sharing information by any means such as orally, sending an email, posting online) to anybody or person.

Inadvertent Disclosure: Type of incident involving accidental exposure of information to an individual not authorized access.

Personal Information: Personal Information is recorded information about an identifiable individual. Refer to MFIPPA, Section 2 (1) for additional information. https://www.ontario.ca/laws/statute/90m56

Personal Health Information: Personal Health Information is identifying information about an individual that relates to their health or providing health care to the individual. Refer to PHIPA, Section 4 for additional information: https://www.ontario.ca/laws/statute/04p03

Privacy Breach: The improper or unauthorized creation, collection, use, disclosure, management, retention, or disposition of Personal Information.

Privacy Breach Investigation: It is a process to identify and analyze the events with stakeholders that led to a privacy breach.

Privacy Breach Investigation Report: Privacy Unit assesses the cause of a privacy breach and reviews all applicable policies and practices. The Privacy Unit consults with stakeholders and releases this Report with privacy analysis and recommendations in regard to protecting personal information, privacy breach response plans and staff training.

Privacy Incident: Any occurrence that impacts or has the potential to compromise personal information or data under City's custody or control.

Risk Management Plan: A report that identifies how a project sponsor will accept, avoid, or reduce the privacy risks identified for a technology, system, program, or service.

Unauthorized Access: The collection, use or disclosure of personal information without the consent of individuals and for purposes that are not permitted or required by the MFIPPA.

Use: The purpose(s) for which the information was obtained or compiled.

Appendix B: Checklist

Step 1: Prepare

- ☐ Designate a privacy breach point of contact within your Division or Unit
- ☐ Ensure appropriate staff complete privacy awareness and training
- ☐ Restrict access to Personal Information
- ☐ Create processes that ensure Personal Information is collected, used, disclosed, and disposed of in accordance with legislation
- ☐ Have appropriate staff, vendors or contractors review and understand this protocol

Step 2: Detect, Analyze and Report

- ☐ Ensure appropriate staff within the City are immediately notified of the breach, including CIMS' Privacy Unit (privacy@toronto.ca)

Step 3: Contain and Eradicate

- ☐ For cyber incidents, identify the scope of the potential breach with the OC and take steps to contain and eradicate it. Reference: Cyber Incident Response Plan.
- ☐ For physical breaches, contact and work with Divisional staff or Corporate Security to contain the breach (depending on the location, severity and scale).

Step 4: Investigate and Document

- ☐ Divisional / Unit complete and submit a Privacy Breach Investigation Questionnaire to the Privacy Unit (privacy@toronto.ca) to capture some descriptions about the privacy incident/breach, such as date and location of the incident, how was the incident discovered.
- ☐ Privacy Unit will conduct a preliminary assessment and determine whether:
  - a privacy breach occurred;
  - a Privacy Breach Investigation Report is required;
  - to notify IPC and/or affected parties if applicable
- ☐ Privacy Unit, with the Division's support, may draft a Privacy Breach Investigation Report to provide privacy analysis and key recommendations.

Step 5: Notify Affected Parties (where applicable)

- ☐ The Privacy Unit, in collaboration with the Division and Legal Services, will determine if a Notice to Affected Parties is required
- ☐ Division to draft a Notice of Affected Parties and Division to send out notice to effected parties.

Step 6: Notify IPC (where applicable)

- ☐ The Privacy Unit, in collaboration with the Division and Legal Services, will determine if IPC to be notified of breach
- ☐ The Privacy Unit, when appropriate and in collaboration with the Division and Legal Services, notifies IPC of breach in writing

Step 7: Mitigate and Prevent

- ☐ Privacy Unit outlines required mitigation tactics in Privacy Breach Investigation Report or communications.
- ☐ Division sign-off on the Privacy Breach Investigation and accept privacy risks and mitigation tactics identified
- ☐ Division implements mitigation tactics outlined in the Privacy Breach Investigation Report
- ☐ Division documents the implementation of each risk mitigation action

Step 8: Log and Retain Records

- ☐ Privacy Unit maintains a log of all privacy breaches and recommendations
- ☐ Privacy Unit retains copies of all artifacts produced during the investigation in accordance with the City's Records Retention By-law (retention code G0265)