
Privacy Incident Handling Procedure

[DRAFT]

Procedure No:	6700-PR2
Version:	3
Policy Reference	6700 Access and Privacy Program Management
Category:	Administrative
Approval Body:	Board of Governors
Executive Sponsor:	VP People, Culture, Inclusion (PCI)
Entity Responsible:	Information Access and Privacy Office (IAPO)
Directory of Records:	0650-15
Classification:	Information Management
Approval Date:	2026 Mxx DD [tbd]

Overview

In accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and Policy 6700 Access and Privacy Management Program, this Procedure establishes a clear and consistent process for identifying, reporting, assessing, containing, evaluating and responding to Privacy Incidents and Privacy Breaches.

Following evaluation, a Privacy Incident may be determined to be a Privacy Breach, occurring when Personal Information has been *confirmed* to have been accessed, collected, used, disclosed, modified, or disposed without authorization by BCIT policy or under FIPPA.

Objectives

In addition to guiding management of Privacy Incidents, this Procedure assigns roles and responsibilities and supports compliance with Privacy Incident notice requirements.

Application

This Procedure applies to all BCIT Employees and Service Providers (it applies only during the term of Service Providers' engagement with BCIT).

Service Providers must comply with all applicable Privacy Incident reporting, response, notification, and related requirements, including those set out in any contract, Privacy and Data Security Schedule, service agreement, memorandum of understanding, or other arrangement governing the services provided to BCIT.

Related Documents and Legislation

Provincial Legislation

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/2012.

BCIT Policy

6700 Access and Privacy Management Program

Related Reference

Office of the Information and Privacy Commissioner for British Columbia. (2023). Privacy Breaches: Tools and Resources for Public Bodies. (Guidance Document 2584)

Definitions

The definitions in Policy 6700 Access and Privacy Management Program apply to this Associated Procedure, as well as the additional terms below:

Privacy Incident means any actual, suspected, attempted, or potential event involving Personal Information that affects, or may affect, the confidentiality, integrity, or availability of Personal Information in BCIT's Custody or Control. Privacy Incidents may result from human error, system failures, cybersecurity incidents, procedural deficiencies, or deliberate actions by internal or external parties.

Privacy Incident Report Form is a formal record documenting the key details of a Privacy Incident, including the individuals affected, the type of Personal Information involved, the cause and scope of the Incident, and the actions and safeguards implemented to contain and mitigate the Incident.

Privacy Incident Response Protocol means the formal process used by the IAPO for managing and responding to a Privacy Incident.

Guiding Principles

- Privacy Incidents must be addressed promptly to contain risks, limit exposure, and reduce potential harm to affected individuals. Responses should be coordinated, documented, and escalated as appropriate, with clear accountability for containment, notice, mitigation, and oversight.
- Decisions relating to the assessment of and response to Privacy Incidents are guided by the sensitivity of the Personal Information involved, the potential impact on individuals and BCIT, and applicable legal, regulatory, policy, and contractual requirements. Affected individuals, regulators, and Service Providers will receive timely notice where required.
- Privacy Incidents are reviewed by the IAPO to identify causes, support corrective action, strengthen controls, and reduce the likelihood of recurrence.
- Protecting Personal Information is a shared responsibility across BCIT, supported by training, awareness, and clear procedures.

- When managing and responding to Privacy Incidents, BCIT considers the diverse needs and experiences of affected individuals and communities to ensure equitable, accessible, inclusive, and respectful response, communication, and mitigation efforts.

Procedure

Stages below may occur sequentially or concurrently and may overlap depending on the Privacy Incident. Upon a person becoming aware of a Privacy Incident, the following steps are to be followed without delay:

1. Step One: Identify, Report, Contain, and Document

Identify

Early identification of a Privacy Incident supports effective containment, mitigation, and response. Examples of Privacy Incidents may include, but are not limited to:

- Unauthorized access to records, systems, or databases.
- Disclosure of Personal Information to an unauthorized recipient or misdirection to an unintended (wrong) recipient (e.g., by email).
- Failure to securely store, transmit, or dispose of Records containing Personal Information.
- Suspected or confirmed theft, loss, compromise, or unauthorized alteration of Personal Information.
- Ransomware, phishing, or other cybersecurity incidents involving Personal Information.
- Theft of an issued device such as a laptop or phone.

Report

Employees who become aware of, suspect, or identify a Privacy Incident must promptly notify their manager or supervisor and the IAPO at privacy@bcit.ca. The Business Owner will then be informed and engaged, as appropriate.

Contain

The Privacy Officer, Manager, designated employee, and, if appropriate, the Business Owner, will take immediate steps to contain known Privacy Incidents and limit them. Information Technology Services, the Cyber Security Office, and other Business Owners will support as needed.

Containment focuses on stopping the unauthorized collection, access, use, disclosure, alteration, or disposal of Personal Information; recovering information where possible; securing affected systems and Records; and implementing preventative safeguards. Every reasonable effort will be made to reduce the risk of harm to affected individuals while preserving evidence needed for investigation and remediation.

Containment may include:

- Recalling an email or communication sent in error.

- Stopping the activity that led to the Incident.
- Recovering Personal Information, records, devices, or equipment.
- Restricting or disabling access to affected systems, applications, or accounts.
- Revoking, disabling, or resetting user credentials.
- Correcting physical or technical security weaknesses.
- Implementing temporary safeguards to prevent further unauthorized access, use, or disclosure.
- Preserving relevant Records, logs, and other evidence.

Document

IAPO will establish and maintain a Privacy Incident file. The file will document the known facts of the Privacy Incident, containment measures, risk assessment, decisions regarding notice, and actions taken to mitigate risks and prevent recurrence. IAPO retains Records related to Privacy Incidents in accordance with the Directory of Records.

2. Step Two: Risk Evaluation

Upon receiving a report of a Privacy Incident, the Privacy Officer will determine its nature and scope and whether a Privacy Breach has occurred.

As part of the assessment, the Privacy Officer determines whether the Privacy Incident or Privacy Breach poses a risk of significant harm to affected individuals. This assessment will consider, at a minimum, the sensitivity of the Personal Information, the likelihood of unauthorized collection, access, use, or disclosure, the potential for misuse, and whether the Personal Information has been fully recovered or otherwise secured.

Significant harm as defined in FIPPA includes:

- Identity theft
- Bodily harm
- Humiliation
- Damage to reputation or relationships
- Loss of employment, business or professional opportunities
- Financial loss
- Negative effects on a credit record
- Damage to or loss of property

The results of the risk assessment will inform next steps, mitigation measures, and decisions about notice.

Depending on the assessed level of risk, the Privacy Officer may establish a Privacy Incident response team for Incident management: its composition is determined based on the nature, scope, and complexity of the Incident.

For example, in assessing potential harm, BCIT will consider whether the incident may have disproportionate impacts on individuals or groups based on accessibility needs, Indigenous identity, racialized identity, gender identity, or other relevant factors.

3. Step Three: Notice

In determining whether notice is required, the Privacy Officer considers the nature of the incident; the type and amount of Personal Information involved; and the potential for harm to affected individuals.

Decisions regarding notice are documented in the Privacy Incident file, including whether to notify affected individuals, the Office of the Information and Privacy Commissioner, and other appropriate parties.

If the Privacy Officer determines that notice is required, BCIT will make reasonable efforts to notify affected individuals at the earliest opportunity, relative to the circumstances of the Incident.

Notifications should be provided in accessible formats and through appropriate communication methods to accommodate the needs of affected individuals. Where appropriate, alternative formats, plain language communications, language interpretation, translation services, or other accessibility supports may be used.

Under the direction of the Privacy Officer the Business Owner or designate shall notify affected individuals directly, in writing, unless the conditions for indirect notice under section 11.1(2) of the *FIPPA Regulation* are met.

Notice to affected individuals should include:

- The date on which BCIT became aware of the Privacy Incident.
- A description of the Privacy Incident, including:
 - The date or period during which the Incident occurred.
 - The Personal Information involved.
 - How the Incident occurred and how it was discovered.
- A description of the steps taken by BCIT to contain the incident.
- A description of any potential risks or harms to affected individuals.
- Steps that individuals can take to reduce the risk of harm.
- Contact information for a BCIT representative who can respond to questions.
- Information about the individual's right to contact the Office of the Information and Privacy Commissioner.

The Privacy Officer will notify the Head and summarize the risk of harm and any recommended notifications and mitigation measures. Where required by section 36.3 of FIPPA the Privacy Officer will notify OIPC.

4. Step Four: Security Safeguards and Prevention Strategies

To strengthen the protection of Personal Information and make future Incidents less likely, the Privacy Officer, in consultation with relevant departments and Business Owners, will ensure that administrative, technical, and physical safeguards are reviewed and enhanced to address identified risks.

Prevention and mitigation measures may include, but are not limited to:

- Identifying, analyzing, and addressing the causes of the Incident, including gaps in processes, systems, or practices.
- Reviewing and updating:
 - Privacy Risk Assessments.
 - Collection Notices.
 - Contractual arrangements with Service Providers and third parties.
- Enhancing access controls, system monitoring, encryption, and documented procedures.
- Strengthening physical security measures where applicable.
- Requiring Employees to complete privacy and security awareness training.
- Verifying that Service Providers and third parties have implemented corrective actions.

The Privacy Officer may recommend organizational improvements to the Head based on learning from the Privacy Incident.

Duties and Responsibilities

Privacy Officer

The Privacy Officer (or designate) will:

- Refer to the Privacy Incident Protocol as a guide to handling Privacy Incidents.
- Assess reported Privacy Incidents and determine their nature, scope, extent, and whether Personal Information is involved.
- Lead and coordinate the Privacy Incident response, including documenting decisions, actions taken, and timelines.
- Assess the risk of significant harm to affected individuals under section 36.3 of FIPPA, considering the sensitivity of the Personal Information and the likelihood of misuse.
- Notify and engage relevant departments and Business Owners to support containment and mitigation.
- Determine whether notifying OIPC is required and ensure such notice is in accordance with FIPPA.
- Determine whether affected individuals will be notified, and provide direction to regarding the content, timing, and method of notification.
- Determine whether external authorities such as law enforcement or regulators will be notified.
- Ensure administrative, technical, and physical safeguards are implemented or strengthened.
- Report findings, risk assessments, and outcomes to the Head as needed.
- If warranted, inform the President and Senior Leadership of the Incident.

Manager

Managers are responsible for coordinating an appropriate response to Privacy Incidents. They will:

- Ensure Employees are aware of and comply with Policy 6700 Access and Privacy Management Program, this Procedure, and Privacy Incident reporting requirements.

- Support prompt reporting, investigation, notification, and mitigation.
- Ensure corrective actions are implemented.

BCIT Employees

Employees play a critical role in Privacy Incident responses. They will:

- Become familiar with their responsibilities under Policy 6700.
- Take steps to Protect Personal Information in their Custody or Control.
- Promptly report any actual or suspected Privacy Incidents to their Manager.
- Cooperate fully in Privacy Incident investigations and responses.
- Complete required privacy and information security training.

Associated Forms

BCIT Privacy Incident Report Form

Appendix

None

Approval History

		<u>Approval Date</u>	<u>Status</u>
Created:	Procedure 6700-PR2 version 1	2012 May 12	Replaced
Revised:	Procedure 6700-PR2 version 2	2021 May 21	In Force
Revised:	Procedure 6700-PR2 version 3 [Draft]	2026 Mmm dd [tbd]	pending

Scheduled Review Date

yyyy Mmm dd [tbd - upon executive or Board approval]; however, the Policy's Executive Sponsor may initiate review at any time.