Privacy Incident Response

Procedure No:	6700-PR2
Version:	2
Policy Reference:	6700 - Freedom of Information and Protection of Privacy
Category:	Information Management
Approving Body:	Board of Governors
Executive Sponsor:	VP Human Resources & People Development
Department Responsible:	Information and Privacy Office
Directory of Records Class:	0650-15
Approval Date:	2021 May 26

Objectives

This procedure applies directly to Policy 6700, Freedom of Information and Protection of Privacy.

The purpose of this procedure is to establish the framework for responding to an actual or suspected privacy incident.

Table of Contents

Application and Scope of this Procedure

This Procedure applies to all BCIT employees, service providers and volunteers.

With respect to service providers, this procedure applies only during the term of their contract with BCIT.

Definitions

Definitions in Policy 6700, Freedom of Information and Protection of Privacy apply to this procedure.

information security incident: has the same meaning as in Policy 3502, Information Security i.e. an identified occurrence of a system, service or network state indicating an actual, possible, or

pending breach of information security or acceptable use polices, or a failure of safeguards, or a previously unknown situation that may be security relevant.

personal information: has the same meaning as in the Act, i.e. recorded information about an identifiable individual other than business contact information.

privacy breach: means a confirmed case of unauthorized access, collection, storage, retention, disposition, use or disclosure of personal information to which the Act applies. Such activity is unauthorized if it occurs in contravention of FIPPA or BCIT Policy 6700 Freedom of Information and Protection of Privacy. Examples of a privacy breach include but are not limited to the following:

- The collection and use of personal information when there is no demonstrable need for it to administer a BCIT sanctioned program or activity.
- Unauthorized access to and use of personal information by an employee outside the performance of their assigned duties.
- An email message or its attachment containing personal information addressed and sent to the wrong person(s).
- Disclosure of personal information to an unauthorized third party.
- The use of a software application or service provider who stores an individual's personal information outside Canada without the individual's prior express written consent or other legal authority stipulated under the Act.
- The unauthorized copying, removal, and retention of personal information in records belonging to BCIT..
- An information security incident involving personal information such as names, unique identifiers when unwanted or unexpected events threaten privacy or information security that can be accidental or deliberate and include the theft, loss, alteration, or destruction of information.

privacy incident: means an actual, possible, or pending privacy breach.

unauthorized disclosure: means the disclosure of, production of or the provision of access to personal information to which the *Freedom of Information and Protection of Privacy Act* (FIPPA) applies, if that disclosure, production, or access is not authorized under FIPPA.

Procedure

There are several stages when responding to a privacy incident. These stages may occur sequentially or concurrently and may overlap depending upon the nature of the privacy incident.

Identification and Reporting

Privacy incidents may be identified at any level through following situations.

- A complaint or concern involving the collection, use, disclosure or security of personal information.
- Monitoring the use of a BCIT system.
- Review of a current or proposed business practice or activity involving access, use, or disclosure of personal information in the custody or control of BCIT.
- In accordance with Policy 3502 Information Security, a report of the loss or theft of an Information Asset containing personal information.

- In accordance with Policy 7170 Safety and Security, the loss or theft of a BCIT asset or device containing personal information.
- Report from an external source such as a BCIT service provider or other third party.

Individuals who are aware of or suspect a privacy incident has occurred or is likely to occur must immediately notify the Information Access and Privacy Office (IAPO) at email: privacy@bcit.ca using the subject line – "**Privacy Incident**". It is recommended that individuals follow the steps set out in the Privacy Incident Checklist created by IAPO.

If the incident is related to BCIT information technology resources, the individual must copy (Cc:) the email to the IT Service Desk at techhelp@bcit.ca.

If the incident is related to BCIT campus safety and security, the individual must copy (Cc:) the email to Safety, Security and Emergency Management at safety@bcit.ca.

Initial Assessment

As soon as possible, IAPO will conduct an initial assessment of a privacy incident, including but not limited to the cause, severity, and associated risk, then determine further actions.

Where there has been a report to IAPO of an unauthorized disclosure of information involving BCIT information systems, the Privacy Officer will inform the Chief Information Officer or designate.

Where IAPO determines that the suspected incident is within the mandate and/or jurisdiction of another Administrative Authority, IAPO will notify that Administrative Authority.

If the Privacy Officer determines that there may be or has been a substantial privacy incident they will inform the Vice-President Human Resources & People Development and may notify the President as appropriate.

The Privacy Officer may consult with the Office of the Information and Privacy Commissioner (OIPC) regarding relevant reporting obligations.

Containment

Employees who identify a privacy incident are responsible for making reasonable efforts to immediately contain the incident and limit any breach. For example, if they are technically able to or can call for assistance to:

- stop the unauthorized practice;
- recover record(s) or information that has been improperly collected, used, disclosed, or disposed of;
- revoke or change an individual's access to the electronic system or database;
- changing a password to a protected file or server; or
- correct weaknesses in physical or cyber security.

Risk Assessment

Upon being notified that a privacy incident has occurred or that a privacy incident is suspected or is likely to occur, the Privacy Officer may assemble a response team, which may include but is not limited to the following (or their designates).

- Director, Corporate Services
- Director, Cyber Security
- Director, Enterprise Risk & Internal Audit
- Director, Marketing and Communications

- Director, Safety, Security and Emergency Management
- Administrative Authorities responsible for the personal information involved (e.g. for employee information, Director, Employee Relations; for student information, the Registrar)

Where a response team is formed, the team will confer to review and investigate the reported incident and determine if the incident is a privacy breach and if so, whether it is an isolated incident or a systemic breach. Steps may include but are not limited to:

- confirming the personal information involved;
- determining the cause and extent of the privacy incident; and
- assessing the risk to affected individuals and BCIT posed by the privacy incident.

In consultation with the response team, the Privacy Officer will determine the scope and nature of notification.

Notification

In the event that the Privacy Officer has determined notification is required, IAPO will oversee and coordinate any notification to affected individuals and/or third parties.

Follow up and Prevention

Efforts to prevent future breaches will take into account the significance of the breach and whether it was systemic or an isolated instance. The Privacy Officer will identify whether other actions are required to remedy the effects of the breach, such as employee privacy and security awareness education and training, a security audit of physical and/or technical security, or a review of records retention policies and practices and service delivery partners.

The Privacy Officer may also identify other institutional process deficiencies that must be addressed. Affected business areas will work with IAPO or other members of the response team to ensure business processes are modified to prevent similar breaches.

Forms Associated with This Procedure

Privacy Incident Checklist
Privacy Incident Report form

Amendment History

		Approval Date	Status
Created:	Procedure 6700-PR2 version 1	2012 May 01	Replaced
Revised:	Procedure 6700-PR2 version 2	2021 May 26	In Force

Scheduled Review Date

2022 May 26