Privacy Breach

Procedure No.:	6700-PR2
Policy Reference:	6700
Category:	Information Management
Department Responsible:	Privacy and Records Management
Current Approved Date:	2012 May 01

Objectives

This procedure is associated with BCIT policy 6700, *Freedom of Information and Protection of Privacy*.

This procedure will provide guidance to BCIT employees on the process to follow should a privacy incident or breach occur. All staff are obligated to report discovered privacy breaches; departments and individuals have responsibilities, and timelines given in this procedure must be followed.

Table of Contents

Who Does This Procedure Apply To?

This Procedure applies to all BCIT Employees

Definitions

Privacy breach
Privacy breach: an incident in which there is unauthorized access to, collection, use, disclosure, or disposal of personal information by BCIT, its vendors, or its employees. Activities are unauthorized if they contravene BC's *Freedom of Information and Protection of Privacy Act* or BCIT's related policy 6700 and associated procedures. Such breaches may be the result of theft, inadvertent behavior, or advertent behavior. Examples include stolen computers containing personal information of BCIT students or employees, personal information emailed to the wrong organization or person, lost memory devices that contain personal information, and other situations.

Procedure

Identifying Privacy Breach
Privacy incidents maybe identified through any one of the following ways:

- Responding to a personal information usage or privacy complaint
- Monitoring systems on campus
- Responding to an information security breach
- Reporting from an external source

Employee, Supervisor, or Service Provider
An employee or service provider who is made aware of any privacy incident or privacy breach must immediately notify their direct supervisor or director/dean. The supervisor or director/dean will report the breach to the Privacy Manager, who informs the President when the magnitude of the incident warrants.

As well, the supervisor or director/dean should immediately take action to contain the breach if technically able to, or call for assistance to do so. Refer to Appendix 2 – Action Plan.

President
The President will determine which BCIT employees to delegate for the assessment and resolution of the privacy incident. The delegated employees will be chosen from one or more of the following positions and departments:

- Manager, Privacy and Records Management, Library Services
- Chief Information Officer, ITS
- Information Security Officer, ITS
- Director, Safety, Security and Emergency Management
- Director, Supply Management (representing Risk Management)
- Director, Marketing and Communications
- Department(s) and employee(s) where the incident occurred, and departments affected by the incident
- Outside agencies, as necessary.

The President will create a Privacy Incident Task Force comprised of the employees representing the departments necessary for the assessment and resolution of each specific privacy incident. A Lead Investigator will be appointed to chair the Task Force. The President can also be a member of the Task Force if necessary.

Privacy Incident Task Force
The Task Force will:

- Conduct an assessment to determine the nature and scope of the privacy incident
- Take actions to immediately contain the privacy incident (e.g., stop the practice, shut down affected systems, revoke access, correct weaknesses in physical security, etc.)
- Conduct a risk assessment
- Produce reports and assessment records that will be maintained in the Privacy and Records Management office
- Determine the communications necessary and the internal and external reporting requirements
- Determine the notifications necessary and produce such notifications (refer to Appendix 1 – Components of a Notification Letter)
- Ensure that BCIT's business practices are improved where necessary to prevent such

Procedure

future incidents
- Take any other actions that arise from specific incidents (refer to Appendix 2 – Action Plan)
- Complete the Privacy Breach checklist (Appendix 3).
- Finalize the process with the conclusion of the internal and external reporting.

Appendix 1 – Components of a Notification Letter

In the event of a privacy breach, determine who should be notified, and include the following elements in the notification letter:

- Date of the notification letter
- Date the breach occurred
- The department, school, or office in which the breach occurred
- Description and nature of the breach (e.g., computer theft, inappropriate release of information, lost memory device, etc.)
- Description of the information that was stolen, lost, released, etc.
- Risks or possible consequences to the person or group/organization whose information was breached (the "information owner")
- Steps taken so far, and further steps to be taken regarding this incident, to control or mitigate the possible harm
- Further steps planned or in process to prevent future privacy breaches
- Actions the information owner can take to prevent or reduce the possible harm
- Contact information for British Columbia's Office of the Information and Privacy Commissioner
- Contact information for the BCIT Records Management and Privacy Office

Add additional comments (such as regrets) or other relevant information as appropriate.

Appendix 2 – Action Plan

In the event of privacy breach, and considering the nature of the breach, assign the action steps below to the recommended personnel, as appropriate.

	Action Required	Responsibility	Recommended Timelines
1	Contain the breach	Affected program area	Immediate
2	Report the breach within BCIT	Program area staff (report to management and Manager Privacy) Privacy Manager (report to President as necessary)	Day of breach discovery
3	Designate lead investigator. Select Privacy Incident Task Force as appropriate	Privacy Manager or President designates lead investigator	Day of breach discovery
4	Protect and preserve the evidence	Lead Investigator, Privacy Manager	Day of breach discovery
5	Contact RCMP if necessary	Director, Safety, Security, and Emergency Management	Day of breach discovery
6	Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within two days of breach discovery
7	Determine whether to report the breach to the BC Privacy Commissioner	Privacy Manager, in consultation with President and Lead Investigator	Within two days of breach
8	Take further containment steps as indicated by preliminary analysis	Lead Investigator, Privacy Manager	Within two days of breach
9	Evaluate risks associated with breach	Lead Investigator, Privacy Manager	Within one week of breach
10	Determine whether to notify affected parties	Lead Investigator, Privacy Manager	Within one week of breach
11	Notify affected parties as determined	Task Force	Within one week of breach
12	Contact other parties as appropriate	Task Force	As needed
13	Determine whether further, in-depth investigation is needed	Task Force	Within two to three weeks of breach
14	Further investigate the cause and extent of breach if appropriate	Lead Investigator	Within two to three weeks of breach
15	Review investigation findings and improve prevention strategies	Task Force	Within two months of breach
16	Implement prevention strategies/ improvements	Privacy Manager or Program Area Manager	Depends on the prevention strategy
17	Monitor prevention strategies	Privacy Manager or Program Area Manager	Privacy and security audits annually or as scheduled
18	Produce internal and external reports	Task Force, Privacy Manager	After investigations and mitigation is completed

Appendix 3 – Privacy Breach Reporting Form and Checklist

Reporting a Privacy Breach

Internal Reporting

Any privacy breach incident must be reported internally, as indicated in the main body of this procedure and in the Action Plan given in Appendix 2.

For reporting within BCIT, access the fillable form, *Privacy Breach Report and Checklist,* next to this procedure on the BCIT Policy web page. This form may also be used as a checklist to help guide the internal response at BCIT, and to evaluate BCIT's response to a privacy breach incident.

External Reporting

The Manager, Privacy and Records Management in consultation with the Task force will determine when reporting to the Privacy Commissioner is needed.

To determine whether to notify the Office of the Information and Privacy Commissioner (OIPC), the Manager of Records Management and Privacy should consider the following factors (as provided by the OIPC):

- ☐ The personal information involved is sensitive
- ☐ There is a risk of identity theft or other harm including pain and suffering and loss of reputation
- ☐ A large number of people have been or may be affected by the breach
- ☐ The information has not been fully recovered
- ☐ The breach is a result of a systemic problem or a similar breach has occurred before
- ☐ The Institute requires assistance in responding to the privacy breach
- ☐ You want to ensure that the steps taken comply with BCIT's obligations under privacy legislation

To report a privacy breach to the OIPC:

1. Accesses the reporting form ("Privacy Breach Checklist") from the OIPC website via your the preferred link below, and follow the directions given on the first page. The form is available in PDF, and in an MS Word document that can be filled out electronically.

   http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist%28June2008%29.pdf

   http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist%28June2008%29.doc

2. Include a copy of the notification letter sent to the party (parties) whose information was breached. Also include a copy of the audit report, if any. The OIPC website provides additional information, forms, and templates.

Reporting Form Contents

The OIPC reporting form ("Privacy Breach Checklist") asks for most of the following information (numbering differs).

Report Date

Contact Information

1. Name of Organization British Columbia Institute of Technology
2. Department or School
3. Contact Person

- ☐ Name
- ☐ Title
- ☐ Phone Fax
- ☐ Email
- ☐ Mailing Address

Risk Evaluation

Incident Description

1. Describe the nature of the breach and its cause
2. Date of incident
3. Date incident was discovered
4. Location of incident
5. Estimated number of persons affected
6. Type of persons affected
   - ☐ Client/ Customer/ Patient
   - ☐ Employee
   - ☐ Student
   - ☐ Other

Personal Information Involved

7. Describe the type of personal information involved (e.g., name, address, SIN, financial or medical) Do not include any identifiable personal information.

Safeguards

8. Describe the physical security measures used in the location where the breach occurred (locks, alarms, etc.)

9. Describe technical security measures
   - ☐ Encryption
   - ☐ Password
   - ☐ Other (describe)

10. Describe organizational security measures (clearances, policies, training programs, contract provisions)

Harm from the Breach

11. Identify the type of harm(s) that may result from the breach.
    - ☐ Identity theft
    - ☐ Risk of physical harm
    - ☐ Hurt, humiliation, damage to reputation
    - ☐ Loss of business or employment opportunities
    - ☐ Breach of contractual obligations
    - ☐ Future potential breaches due to similar technical failures
    - ☐ Failure to meet professional standards or certification standards
    - ☐ Other (specify)

Notification

1. Has the BCIT Privacy Manager been notified?
   - ☐ Yes Who was notified and when?
   - ☐ No When to be notified

2. Has the BCIT Safety, Security and Emergency Management Department been notified? Did Safety, Security, and Emergency Management notify the RCMP?
   - ☐ Yes Who was notified and when?
   - ☐ No When to be notified

3. Have the affected persons been notified?
   - ☐ Yes Manner of notification
   - ☐ No Why not?

4. What information was included in the notification?
   - ☐ Date the breach occurred
   - ☐ Description and nature of the breach (e.g., computer theft, inappropriate release of information, lost memory device, etc.)
   - ☐ Description of the information that was stolen, lost, released, etc.
   - ☐ Risks or possible consequences to the person or group/organization whose information was breached (the "information owner")
   - ☐ Steps taken so far, and further steps to be taken regarding this incident, to control or mitigate the possible harm
   - ☐ Further steps planned or in process to prevent future privacy breaches
   - ☐ Actions the information owner can take to prevent or reduce the possible harm
   - ☐ Contact information for the British Columbia Privacy Commissioner
   - ☐ Contact information for the BCIT Records Management and Privacy Office

5. Should the Office of the Information and Privacy Commissioner be notified of the breach? Consider the following factors:
   - ☐ The personal information involved is sensitive
   - ☐ There is a risk of identity theft or other harm including pain and suffering and loss of reputation
   - ☐ A large number of people have been or may be affected by the breach
   - ☐ The information has not been fully recovered
   - ☐ The breach is a result of a systemic problem or a similar breach has occurred before
   - ☐ The Institute requires assistance in responding to the privacy breach
   - ☐ You want to ensure that the steps taken comply with BCIT's obligations under privacy legislation

Mitigation and Prevention

1. Describe the immediate steps taken to contain and reduce the harm of the breach (e.g., locks changed, computer access codes changed or privileges revoked, physical security alterations, risk assessment, computer systems shut down)

2. Describe the long-term strategies you will take to correct the situation (e.g., staff training, policy development/awareness, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security)

Lead Investigator, Forms Associated With This Procedure

Privacy Breach Report and Checklist

Amendment History

1. Created 2012 May 01