

Procedure Number:	6751p
Procedure Title:	Privacy Breach Response
Approved by:	Senate
Approval date:	September 21, 2011
Effective date:	September 21, 2011
Review date:	June 2024
Next review date:	June 2026

### 1. Purpose

- 1.1. This Procedure is designed to support Policy 6751.
- 1.2. This Procedure outlines the steps, responsibilities, and timelines for responding to Privacy Breaches.

### 2. Definitions

- 2.1. The definitions in Policy 6751 apply to this Procedure.

### 3. Discovery and Notification of the Privacy Breach

- 3.1. *Responsibility:* Discoverer of the Privacy Breach must notify the employee with the responsibility.
- 3.2. *Timeline:* Immediate upon the breach discovery.

### 4. Internal Reporting of the Privacy Breach

- 4.1. *Responsibility:* Employee with the direct responsibility for the Privacy Breach must notify the following:
  - 4.1.1. Employee’s manager; and
  - 4.1.2. Privacy and Data Protection Officer at [privacy@ucanwest.ca](mailto:privacy@ucanwest.ca).
- 4.2. *Timeline:* Same day as the breach discovery.
- 4.3. If the employee’s manager and the Privacy Data Protection Officer are unavailable, then the employee may seek assistance from the IT department as necessary to contain the Privacy Breach.

### 5. Preserve the Evidence

- 5.1. *Responsibility:* Privacy and Data Protection Officer.
- 5.2. *Timeline:* Same day as the breach discovery.

## **6. Contain the Privacy Breach**

6.1. *Responsibility:* Privacy and Data Protection Officer.

6.2. *Timeline:* Within two days of the breach discovery.

## **7. Evaluate the Risks**

7.1. *Responsibility:* Privacy and Data Protection Officer.

7.2. *Timeline:* Within two days of the breach discovery.

## **8. Designate a Breach Response Team as Appropriate**

8.1. *Responsibility:* Privacy and Data Protection Officer.

8.2. *Timeline:* Within two days of the breach discovery.

## **9. Determine If the Privacy Breach Should Be Reported to the BC Privacy Commissioner**

9.1. *Responsibility:* Privacy and Data Protection Officer (in consultation with the Executive team).

9.2. *Timeline:* Within one week of the breach discovery.

## **10. Contact Police If Necessary**

10.1. *Responsibility:* Privacy and Data Protection Officer (in consultation with the Executive team).

10.2. *Timeline:* Within one week of the breach discovery.

## **11. Determine If Notification of Affected Individuals Is Required**

11.1. *Responsibility:* Privacy and Data Protection Officer.

11.2. *Timeline:* Within one week of the breach discovery.

## **12. Notify Affected Individuals**

12.1. *Responsibility:* Privacy and Data Protection Officer.

12.2. *Timeline:* Within 1 week of the breach discovery.

## **13. Contact Others as Appropriate**

13.1. *Responsibility:* Privacy and Data Protection Officer.

13.2. *Timeline:* As appropriate.

**14. Conduct Further Investigation If Necessary**

14.1. *Responsibility:* Privacy and Data Protection Officer, security officer, external auditor, or investigator.

14.2. *Timeline:* Within 2-3 weeks of the breach discovery.

**15. Review Investigative Findings and Develop Prevention Strategies**

15.1. *Responsibility:* Privacy and Data Protection Officer and program area manager.

15.2. *Timeline:* Within one month of the breach discovery.

**16. Implement Prevention Strategies**

16.1. *Responsibility:* Privacy and Data Protection Officer and program area manager.

16.2. *Timeline:* Depending on approach selected.

**17. Monitor Prevention Strategies**

17.1. *Responsibility:* Privacy and Data Protection Officer and program area manager.

17.2. *Timeline:* Regular privacy audits.

**18. Related Policies**

Policy Number	Policy Title
1506	Survey
2700	Acceptable Use of Information Technology Resources
6750	Records Management
N/A	Website Privacy Policy