UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Procedures

RESPONDING TO A PRIVACY INCIDENT OR PRIVACY BREACH PROCEDURES

Number: GV 2.1
Classification: Governance
Procedural Authority: President
Procedural Officer: Senior Governance Officer
Effective Date: July 31, 2023
Supersedes: NA
Date of Last Review/Revision: July 2023
Mandated Review Date: July 2030

Parent Policy: Protection of Privacy Policy

Table of Contents

1.0 PURPOSE

The purpose of this document is to set out response procedures to be followed when a Privacy Incident or Privacy Breach, which is in contravention of Part 3 of FOIPPA occurs at the University.

2.0 PROCEDURES

2.1 Reporting

2.1.1 Members of the University Community must immediately report all privacy breaches and incidents to the Office of University Governance.

2.1.2 All breaches must be reported by emailing privacy@unbc.ca or calling 960-5850.

2.2 Initial Assessment

2.2.1 Within one business day of receipt of the privacy breach or privacy incident report, a Privacy Officer is assigned to the case and conducts an initial assessment to determine the cause, severity, and risk of the privacy incident or breach.

2.2.2 If the initial assessment reveals that the reported incident is neither a privacy incident nor a privacy breach, the Privacy Officer forwards the report to the appropriate University program or unit lead responsible for the information involved.

2.2.3 If the initial assessment reveals that the incident or breach involves highly sensitive personal information or a substantial number of records, the Privacy Officer must inform the requisite Vice-President (or designate) and may notify the President as appropriate.

2.2.4 If the initial assessment reveals suspected criminal activities, the Privacy Officer must notify the President and appropriate law enforcement authority.

2.2.5 If the initial assessment reveals the unauthorized disclosure or access of information managed by University systems, the Privacy Officer informs the Chief Information Officer.

2.3 Containment

2.3.1 The Privacy Officer coordinates efforts to contain or recover information involved in a privacy breach or privacy incident.

2.3.2 After an initial assessment is complete, the Privacy Officer assembles an appropriate response team including, but not limited to, the following as needed:

i. the individual reporting the privacy incident or breach;
ii. the University program or unit lead responsible for personal information involved;
iii. the dean/director, to whom the program or unit lead reports;
iv. the vice-president overseeing the program or unit involved;
v. the Chief Information Security Officer;
vi. the Chief Information Officer;
vii. the Senior Governance Officer.

2.3.3 The response team must make reasonable efforts to immediately contain or mitigate the impact of the privacy incident or breach, for example:

i. prevent further unauthorized practice(s);
ii. recover records;
iii. correct physical security weaknesses;
iv. reset access permissions;
v. shut down affected systems; and
vi. disable network access of affected systems.

2.3.4 If the incident or breach involves University information systems, the Chief Information Officer (or designate) manages containment protocols for affected information systems.

2.3.5 The response team's efforts to contain the privacy incident or breach must be completed without unreasonable delay and should not normally exceed seven business days.

2.4 Full Assessment and Risk Evaluation

2.4.1 After the response team has initiated containment procedures, the Privacy Officer must begin assessing the impact of the privacy incident or breach by:

i. confirming the personal information involved;
ii. determining whether the incident is a privacy breach;
iii. determining the cause and extent of the privacy incident breach; and

iv. confirming the individual(s) potentially affected by the privacy incident or privacy breach.

2.4.2 The Privacy Officer must make all reasonable efforts to have a full privacy breach risk assessment completed within one business day of completed containment activities.

2.5 Notification

2.5.1 The Privacy Officer must notify the Office of the Information and Privacy Commissioner for British Columbia (OIPC) of any privacy breach involving significant harm, as defined in FOIPPA.

2.5.2 The University program or unit lead responsible for personal information involved in the breach must notify individuals affected by a privacy breach, under the direction of the Privacy Officer.

2.5.3 The contents and method of the privacy breach notice must satisfy the notification requirements outlined in FOIPPA.

2.5.4 All reasonable efforts must be made to provide notice to affected individuals within one business day of the completed privacy breach risk assessment.

2.6 Prevention

2.6.1 Based on the privacy breach risk assessment, the Privacy Officer determines if there is need for an audit of:
i. administrative safeguards (e.g., unit procedures or training);
ii. physical security safeguards; and
iii. technical safeguards

2.6.2 The Chief Information Officer (or designate) manages an audit of technical safeguards for university information systems.

2.6.3 The Privacy Officer is responsible for preparing the final privacy breach report which includes:
i. a summary of any audit findings;
ii. implemented changes and updates to current administrative, physical, and technical safeguards; and
iii. recommended changes to existing safeguards.

2.6.4 The final breach report must be shared with all members of the response team.