a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Office of the University Counsel
6328 Memorial Road
Vancouver, BC Canada V6T 1Z2

Phone 604 822 2451
Fax 604 822 8731
access.and.privacy@ubc.ca

Privacy Fact Sheet

Handling Privacy Breaches

Introduction

1. The purpose of this Privacy Fact Sheet is to explain the process for handling a privacy breach. It must be read in conjunction with UBC's Incident Response Plan, which applies to computer security incidents that affect UBC's information technology facilities, infrastructure or data assets.

2. UBC stores a large amount of personal information about employees, students, and research subjects. Inappropriate use or disclosure of this information may constitute a breach of the *Freedom of Information and Protection of Privacy Act* (FIPPA) and may have a significant, even devastating, impact upon the affected individuals as well as reputational and financial harm to the University.

What is a Privacy Breach?

3. A privacy breach occurs when personal information is accessed, collected, used, disclosed or disposed of without proper authorization. "Personal information" is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.

4. As a general rule, UBC faculty and staff members are authorized to access personal information on a "need-to-know" basis, whereas individuals who are not faculty or staff are only authorized to access personal information under exceptional circumstances. If you are not sure whether access was authorized, you should check with a supervisor or manager, or the Office of the University Counsel.

How to Report a Privacy Breach

5. All UBC faculty, staff, contractors and volunteers have a duty[1] to report suspected privacy breaches to their supervisor or manager, who will then initiate an investigation and report to the following units:

    a. The privacy breach must be reported to the Office of the University Counsel by email or using the UBC Privacy Breach Reporting Form.
    b. If there has been a computer security incident, then it must also be reported to the IT Security Office in accordance with the UBC Incident Response Plan. A "computer security incident" is any event where there is suspicion that confidentiality, integrity or accessibility of UBC electronic data has been compromised, or computer systems or infrastructure is vulnerable to attack.
    c. If there has been a theft or other illegal activity, it must also be reported to Campus Security.
    d. Loss or destruction of devices or equipment must be reported to Safety & Risk Services for insurance purposes.

[1] Section 30.5 of FIPPA

Privacy Breach Management Process

6. The following process describes how privacy breaches are addressed.

Action Required	Position Responsible	Recommended Timelines
1. Contain the breach	Unit/department where breach occurred	Immediate
2. Report the breach within UBC	• Staff: report to manager/supervisor • Manager/supervisor: report to Legal Counsel, Information and Privacy • Legal Counsel: report to Executive as required	Same day as breach discovered
3. Designate Lead Investigator and select breach response team as appropriate	Legal Counsel (in consultation with manager/ supervisor)	Same day as breach discovered
4. Preserve the evidence	Lead Investigator or Legal Counsel	Same day as breach discovered
5. Contact police if considered appropriate by Legal Counsel, Information and Privacy	Lead Investigator or Legal Counsel	Same day as breach discovered
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach
7. Determine if the breach should be reported to the Privacy Commissioner	Legal Counsel (in consultation with University Counsel)	Generally within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Lead Investigator or Legal Counsel	Within 2 days of breach
9. Evaluate risks associated with breach	Lead Investigator or Legal Counsel	Within 1 week of breach
10. Determine if notification of affected individuals is required	Legal Counsel	Within 1 week of breach
11. Conduct notification of affected individuals, if necessary	Legal Counsel or unit/department manager	Within 1 week of breach
12. Contact others as appropriate	Legal Counsel or unit/department manager	As needed
13. Determine if further in-depth investigation is required	Legal Counsel or unit/department manager	Within 2 to 3 weeks of the breach

14. Conduct further investigation into cause and extent of the breach if necessary	Legal Counsel, security officer or auditor/investigator	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	Legal Counsel or unit/department manager	Within 2 months of breach
16. Implement prevention strategies	Unit/department manager (in consultation with Legal Counsel)	Depends on the strategy
17. Monitor prevention strategies	Unit/department manager	Annual privacy/security audits

Privacy Breach Notifications

7. UBC has a legal obligation to notify an affected individual as well as the Information and Privacy Commissioner if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant bodily harm; humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; financial loss; negative impact on a credit record; or damage to, or loss of, property.[2] A privacy breach notification must comply with certain requirements set out in the regulations.[3]

8. Before sending a privacy breach notification, UBC faculty, staff, contractors and volunteers must seek advice from the Office of the University Counsel about whether a notification is required and how it should be worded.

How to Get More Information about Privacy and Information Security

9. More information about privacy is set out in the University's Privacy Fact Sheets.

10. Guidance about information security is found in the University's Information Security Standards.

[2] Section 36.3 of FIPPA
[3] Section 11.1 and 112 of the FIPPA Regulation, B.C. Reg. 155/2012