a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

# INFORMATION SECURITY STANDARD U4
## Reporting Information Security Incidents

### 1. Introduction

1.1 Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental or deliberate attempts to break into systems; purpose or consequence can be from benign to malicious. Regardless, each incident requires a careful response, at a level commensurate with its potential to cause harm to an individual and the University, as a whole, as defined in the UBC Incident Response Plan.

1.2 This document defines standards for Users to report any suspicious incidents relating to the security of UBC Electronic Information and Systems. University IT Support Staff (including both departmental IT and UBC IT staff) are responsible for handling security incidents in coordination with UBC Cybersecurity.

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

### 2. Incidents That Must be Reported

2.1 Users must report the following information security incidents (if there is uncertainty whether a violation has occurred, Users must err on the side of caution and report the incident anyway):

2.1.1 all violations of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems; examples include but are not limited to:

2.1.1.1 use of UBC computing facilities to commit illegal acts;

2.1.1.2 unsolicited or spam email originating from UBC sources;

2.1.1.3 unauthorized access, use, alteration or destruction of UBC Electronic Information or UBC Systems, including but not limited to: software, computing equipment, Merchant Systems, network equipment and services;

2.1.1.4 theft of any UBC Electronic Information whether it be via electronic means or physical theft of any Device containing this information; and

2.1.1.5 loss or theft of any Multi-Factor Authentication Device (MFA Device).

2.1.2 unauthorized wireless access points discovered in either merchant areas or areas accessing, transmitting or storing UBC Electronic Information; and

2.1.3 use of Malicious Code, which may show up as unexplained behavior on desktops, laptops or servers such as webpages opening by themselves, new files or folders appearing on the local hard drive, and lockouts of user accounts.

### 3. How to Report Incidents

3.1 Users must immediately report all suspected information security incidents as follows:

3.1.1 to security@ubc.ca or via phone to the IT Service Centre at 604-822-6141. UBC Cybersecurity will coordinate the incident as required in accordance with the UBC Incident Response Plan;

3.1.2 to their supervisor and University IT Support Staff who are assigned to their unit; and

3.1.3 where the incident involves physical security issues on a UBC campus, in addition to information security issues, to Campus Security.

3.2 It is essential to report incidents immediately, as time is of the essence when dealing with information security breaches and other potentially damaging incidents arising from Malicious Code.

### 4. Related Documents and Resources

UBC Incident Response Plan

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems