Standard for Reporting Information Security Incidents

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Users		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

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 College as defined in the IT Incident Response Plan.

1.2 This document defines standards for Users to report any suspicious incidents relating to the security of College electronic information and systems. College IT Staff are responsible for handling security incidents in coordination with College IT Security Team

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):

a) all violations of Use of Information Technology Resources Policy; examples include but are not limited to:

i) use of College computing facilities to commit illegal acts;
ii) unsolicited or spam email originating from College sources;
iii) unauthorized access, use, alteration or destruction of College electronic information or College systems, including but not limited to software, computing equipment, merchant systems, network equipment and services;
iv) theft of any College electronic information whether it be via electronic means or physical theft of any device containing this information; and
v) loss or theft of any multi-factor authentication device (MFA Device).

b) unauthorized wireless access points discovered in either merchant areas or areas accessing, transmitting, or storing College electronic information; and

c) 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.

d) any notices of vendor/saas security incidents or data breach where College data exists.

3. How to Report Incidents

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

a) to itsecurity@okanagan.bc.ca or via phone to the IT Help Desk at local 4444. IT Security will coordinate the incident as required in accordance with the IT Incident Response Plan;

b) to their supervisor; and

c) where the incident involves physical security issues on a campus, 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.

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*