    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.

3.1 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