The purpose of this memo is to remind all University employees about their legal obligation to protect personal information in the custody and under the control of SFU when such information is stored on mobile digital devices.

Under B.C.’s Freedom of Information and Protection of Privacy Act, employees must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. Personal information means recorded information about an identifiable individual including students, employees, alumni, donors and others. Mobile digital devices include laptop, notebook and netbook computers, iPads and other tablets, iPods, smart phones, USB drives, portable external hard drives and other mobile digital storage media such as CDs and DVDs.

The preferred and recommended option is to store personal or confidential information only on secure University, faculty or departmental data servers.

However, personal information may be stored temporarily on a mobile digital device when there is a demonstrated need to do so. In such instances, and to appropriately manage the risks noted above, all SFU employees using mobile digital devices or digital storage media of any type must apply the following minimum, security standards:

1. Any files containing personal information or confidential University business information must be encrypted and protected with a strong password. For example, files such as spreadsheets, databases, text including Word documents and PDFs, presentations, images and audio/video recordings. In most cases, the most convenient mechanism involves encrypting entire disk images containing information, rather than individual files.


There are also a number of commercially available products that can be used to provide acceptable protection.
Apple iOS devices must use Data Protection; see

Android devices must use the built-in encryption facility; see
http://support.google.com/android/bin/answer.py?hl=en&answer=1663755.

Blackberry devices must use the built-in encryption facility; see

Smartphones without encryption ability must not be used to store SFU personal information or other SFU confidential information.

2. Access to any mobile digital device on which personal or confidential information is stored must be secured with a strong password, which must be required on exit from sleep or screen savers. Numeric passcodes are acceptable for securing smartphones, although stronger passwords should be used where possible. Instructions for applying a strong password can be found at this link
http://www.sfu.ca/itservices/accounts/computing_id/choose-password.html;

3. The mobile digital device must be physically secured at all times; and

4. If a mobile digital device is lost or stolen, the user must notify the Information and Privacy Officer, SFU Campus Security and IT Services as soon as possible after realizing the device is missing.

The reasons for this reminder are the quantity of sensitive third party personal information entrusted to the University’s custody and care, the increased availability of mobile storage devices and a reported privacy breach incident involving an unsecured stolen laptop on which personal information was stored.

The above standard will be part of a comprehensive information security website that the Chief Information Officer currently is developing, which will provide members of the university community with further information and resources about this important topic.

We appreciate your continued vigilance to secure and protect the personal information held by SFU.