PRIVACY MATTERS
@ UBC

PERSONAL INFORMATION (PI)* SECURITY - ON THE MOVE

*Personal Information (PI) is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.

MOBILE DEVICES (INCLUDING LAPTOPS, SMARTPHONES, & TABLETS)

1. Using Mobile Devices to store PI is not recommended. Use a secure alternative such as Virtual Desktop Interface (VDI) or Virtual Private Network (VPN). PI stored on mobile devices must be encrypted – see Encryption Requirements below.
2. Set Screensavers to lock automatically after no more than 30 minutes.
3. Install anti-virus software and configure it to update at least once per day.
4. Contact your IT support unit to learn how to configure your computer's firewall.

Refer to Information Security Standard #07 Securing Computing and Mobile Storage Devices/Media.

ENCRYPTION REQUIREMENTS FOR MOBILE DEVICES STORING PI

Full Disk Encryption is required for the following devices:

1. Laptops
2. Tablets and smartphones
3. Mobile storage devices/media (e.g. USB keys, CDs, DVDs, tapes, portable hard drives)

Refer to Information Security Standard #05 Encryption Requirements.

WORKING REMOTELY

1. Use caution when using public Wi-Fi networks, such as in airports, coffee shops, public libraries, hotels, and cybercafes.
   a. Don't use third-party devices such as kiosks.
   b. Be aware of others looking over your shoulder at your screen.
   c. Don't leave mobile devices unattended.
   d. Connect to myvpn.ubc.ca or myvpn.ok.ubc.ca before starting to browse the Internet.
   e. Do not use public Wi-Fi if you receive a 'certificate error'.
2. Keep mobile devices secure when working from home and ensure PI cannot be accessed by family members.

Refer to Information Security Standard #06 Working Remotely.

SPECIFIC REQUIREMENTS FOR TABLETS AND SMARTPHONES

1. Password/PIN lock must be at least 5 characters long.
2. Enable the following features:
   a. Ability to determine remote location in the event of loss or theft.
   b. Ability to automatically erase data if 10 consecutive incorrect passwords are entered or in the event of loss or theft.

Refer to Information Security Standard #02 Password and Passphrase Protection and Information Security Standard #07 Securing Computing and Mobile Storage Devices/Media for more information.

Contact your it support representative for clarification or assistance with any of the above requirements. For more information on Information Security Standards, please visit www.cio.ubc.ca/securitystandards. Report information security breaches to security@ubc.ca or by phone to the it Service Centre at 604.822.2008.

www.privacymatters.ubc.ca

THE UNIVERSITY OF BRITISH COLUMBIA