PROTECTING PERSONAL or CONFIDENTIAL INFORMATION AWAY FROM CAMPUS

Whenever information relating to VIU business is used outside of the office or the classroom, there is an increased risk of loss or compromise. VIU is required by the *Freedom of Information and Protection of Privacy Act* (FIPPA) to keep all personal information in its custody or under its control safe and secure.

Here are things you can do to protect personal information when working remotely:

Physical Records

• Remove information from the office only if is essential to carry out your job duties and you have authorization from your manager.

• If possible, take copies of physical records and leave the originals in the office.

• Store physical records in a locked filing cabinet or desk drawer that you have sole access to.

• Exercise diligence in relation to your home security (e.g. lock doors and cabinets, activate alarms when away from home). Mobile devices and hard copies of records or files containing sensitive information must be physically secured.

• Avoid leaving documents unattended on a desk or printer.

• Upon returning to campus, return records to their original storage place as soon as possible and destroy copies securely using the shredding services managed by VIU.

• Sensitive personal information should ideally be cross-shredded and electronic files securely wiped from device memory.

Privacy Safeguards

• Avoid leaving your computer screen unattended. Lock the screen or log off.

• If using a home computer that is shared with others in the household, ensure that you limit access to files containing personal information or confidential business information. Keep passwords secure.

• Do not use your personal email as a means to transfer records containing personal or confidential information for work purposes.

• Conduct telephone calls to discuss employment or other matters involving personal information or confidential business information in private and outside the earshot of others.

• When using video conferencing:

− If you want to record a video conference, say for note-taking, you must have permission from everyone on the call.

− Personal or sensitive business information should not be discussed in public places or in spaces that may include other members of your household.

− Ensure that any visible personal or confidential data is kept away from camera view.

− Cameras and microphones should be turned off when not in use.

• Securely remove all VIU information from a personal computer once no longer needed.

• When using VIU administrative systems remotely, be sure to use a private or incognito browsing window. Systems like SRS and any VIUWEB application can access sensitive information and documents. A private or incognito browsing window will not cache pages or the documents you view from these applications.

Data Breach

All records relating to VIU business are subject to the access and privacy provisions of FIPPA even if they are created, sent, or received through non-VIU email accounts, or stored on personal devices.

If VIU records are lost or stolen:

1. immediately notify your manager; AND
2. report the loss by email: FIPPA@VIU.ca

If a VIU device is lost or stolen:

1. immediately notify your manager; AND
2. report the loss by email: FIPPA@VIU.ca; AND
3. notify the IT Help Desk at 250-740-6300 or email: ithelp@VIU.ca

The Privacy Officer will advise what next steps should be taken.

Working Remotely and Securely

At VIU, we all have a shared responsibility to protect personal and confidential information about students, faculty, staff, alumni, and donors. By taking a few simple steps to stay secure, we all can make an impact on privacy and information security. VIU employees are reminded that all VIU policies and procedures must be followed regardless of their working location.

Information Security Guidelines

• When connecting to VIU resources outside the office, use a VPN connection only for those services that require it.

o Services that DO require the use of VPN include: files on network shares (U drive, department drives).

o Services that DO NOT require the use of VPN include: most VIU resources such as Email, VIU Learn, FRS, Unit 4, SRS, InVIU, VIUTube, all websites.

o Ensure that you have applied all security updates and have updated virus/malware protection if connecting from a personal device. (VIU owned/managed devices are updated automatically). This is critical to protect VIU data.

• Do not accept software updates that are triggered from a website or email, such as Java or Adobe Flash.

• Store your electronic device(s) in a secure location when transporting or travelling (e.g. trunk of a car);

• Avoid using public charging stations (i.e. where a charging dock or cable is already provided), such as on a ferry or in an airport, as these are not considered safe for use.

Be Cyber-Aware: Never Open Unexpected Attachments – Be Careful What You Click

Many attempted phishing and ransomware attacks appear in your inbox looking like an email from a person or service that you trust. If it looks unusual, feels unexpected, has any typos, or it just seems "odd", then do not click any of the links.

One way to verify the link before you click it is to hover over a hyperlink in your inbox, without clicking. When you hover over a hyperlink, you'll see the target URL in the lower-left corner of your browser.

If you can, call the person or business at a phone number that you trust and ask them if the suspicious email is valid. This gives you a second method of communication to verify the email.

Responding to Information Security Concerns

If you have clicked on a deceptive link and provided your credentials, change your password immediately.

If you clicked a suspicious link or if you believe your computer may be compromised, immediately report the concerns by:

• Notifying the IT Help Desk at 250-740-6300 or email: ithelp@VIU.ca.