**DO**

- Read the UBC IT guide to working off campus for reminders regarding collaboration tools and video conferencing platforms.
- Make sure you understand and follow UBC’s Securing Computing and Mobile Storage Devices policy. This includes the newly mandated minimum cybersecurity controls.
- Use approved methods to share files. Be mindful of distribution and dissemination even when utilizing agency-approved platforms.
- Log off of your myVPN connection when away from your computer.
- Follow UBC policy for encrypting computers used for UBC business.
- Use a strong password for your CWL, and change it frequently.
- Close all non-work related windows and applications before and during work related use of personal equipment.
- Create a separate user profile with minimal privileges for work-only use when using a personal computer to perform UBC business.
- Clear browser cache when switching from work to personal use when using a personal computer to perform UBC business.

**DON’T**

- Print work-related materials at home, unless explicitly approved by your manager.
- Auto-forward your office phone to a personal number unless explicitly approved by your manager.
- Connect to phone or video conferences unless you were invited. Upon connecting, always announce your name and affiliation.
- Forward work emails from your FASmail account to a personal email account.
- Connect to a network that you do not own and control (e.g. public Wi-Fi).