Loaner Device Program

Security Recommendations

UNIVERSITY OF TORONTO

✓ DO

- Before you travel, carefully consider what data you need. Bring the minimum.
- Pre-load presentations onto devices to limit accessing U of T's network while traveling.
- Use multifactor authentication (MFA) to access devices and accounts when available.
- Turn off automatic connection capabilities to ensure your devices do not connect or pair with unknown devices or unsecure networks.
- Disable features such as Bluetooth and location services.
- Always maintain control of devices and chargers (e.g. at airports, restaurants, conferences, hotels). If you must leave a device unattended, if possible, take the battery and SIM card with you.
- Keep your devices as carry-on items.
- Power off devices while going through customs or other inspection points. Make sure the device's battery is fully charged in case you are asked to prove the device is functioning properly.
- Print boarding passes to avoid turning your device on while at customs or other inspection points.
- Secure your cables, chargers and peripherals. Modern cables can be programmed to compromise your device since they can contain microcontroller components.
- Fully shut down, and power off your devices every night.
- Assume that communications transmitted over public carriers can be intercepted.

🚫 DON'T

- **DO NOT** connect to Bluetooth or Wi-Fi networks while traveling, even secured networks. Wi-Fi should only be used to hotspot the issued laptop off of the issued cellphone.
- **DO NOT** download or access social media accounts. **DO NOT** download new applications.
- **DO NOT** send information between your personal and work devices. This creates a link.
- **DO NOT** keep or reuse passwords on your devices.
- **DO NOT** tell external contacts that you have loaner devices. Instead, they are your work devices.
- **DO NOT** plug in or connect your devices to any non-issued devices (e.g., USB / USB-C sticks, memory cards, chargers, cameras, computers, photocopiers, fax machines, digital picture frames, etc.).
- **DO NOT** access cloud data storage sources.
- **DO NOT** open emails, attachments or click on links from unknown sources.
- **DO NOT** use Remember Me features on websites.
- **DO NOT** use Biometric log-in services on your devices .

UPON RETURN

- Leave devices on airplane mode and return them to the Digital Workplace Team. Do not delete content, software or logs off your device.
- Change your UTORid password.
- Report any unusual behavior, such as performance issues, pop-ups, reduced battery performance, overheating of your devices or suspected security concerns, such as devices inspected by border / government officials.