Best Practices for IT Security during International Travel

The Department of Commerce, the Department of State, and the Department of Treasury promulgate and enforce regulations that restrict items which a traveler may take on international travel. These items include common items such as laptop computers, smart phones, tablets, blueprints, drawings, technical data, and even encryption products.

University employees and students—including you—are subject to these regulations! Failure to comply with these regulations may have serious consequences for the individual who is travelling and the University.

To ensure that an individual does not run the risk of unlawfully releasing controlled technology when traveling internationally, keep the following guidelines in mind:

- Verify that your technology or information falls into one or more of the following categories prior to travelling to non-embargoed countries:
    - Research results that qualifies for the fundamental research exclusion
    - Public domain information
    - Issued patents and published patent applications

- Remove information and software from any electronic device that is export-controlled technical data/information or anything you wish to keep confidential prior to leaving the United States.
    - Deleting a file is NOT enough. Use a “shredder” program to erase the information you do not want to share so that it cannot be recovered.

- When accessing WVU e-mail, use the web-based Office 365 client.
    - The desktop client and mobile applications download all e-mail and attachments to the local device which makes accessing e-mail much more risky while traveling abroad. Do no open any e-mail attachments you suspect contain may export controlled information.

- Take a ‘Clean’ Laptop and Phone
    - If you can, take a device with just the files and applications you will need while traveling. Make sure all software is fully up to date and appropriate security software is installed and activated. Take a prepaid cellphone with only the contact information you will need. Cover laptop cameras when not in use.
    - Assume that any and all information on your computer, tablet and cell phone will be compromised.

- Use Encryption
    - Apply a full disk encryption solution such as BitLocker, FileVault or TrueCrypt. Do not take the encryption keys/recovery disks with you. Encryption provides substantial protection should your laptop, smartphone, or other mobile device become lost or stolen. Be aware that some countries have encryption import restrictions that prevent you from encrypting data on your device.

- Change Your Passwords
    - Change any passwords that you expect to use while traveling. Change the passwords again from a trusted device upon your return.

- Use a Temporary Mail Account
    - If possible, use a temporary mail account through a service such as Gmail, Outlook.com, or Yahoo. If the service supports two-factor authentication, please take advantage of the stronger authentication. Don’t email sensitive information from any device.

- Maintain Control of Your Devices
    - Use strong passwords on all devices. Keep electronic devices on your person or locked up when travelling. Electronic devices are often targeted for theft.

- Disable Unused Services
  - Disable Bluetooth, Wi-Fi, GPS, etc. when not in use to limit avenues of unauthorized access to your device(s).

- Internet Access
  - Public/Hotel networks may be monitored. In some countries, all Internet traffic may be monitored. Assume your Internet traffic is not private.

- Removable Media
  - Do not accept USB drives, SD cards, CDs/DVDs, or other removable media. Do not use any removable media that you've found. Such devices may contain malware. If you connect your USB drive, SD card or external drive in another individuals computer (e.g. for a presentation), consider it compromised and don't reconnect it to your computer.

- Public Charging Stations
  - Do not use USB-based public battery charging stations. The USB interface to your device may be used to deliver viruses or malware.

- Wipe Devices When You Return
  - Treat devices as if they've been fully compromised. Upon your return, do not connect the device to any network. Have your IT department remove important data and wipe/reset electronic devices.

- If an export-controlled item or electronic device is lost or stolen, immediately notify the Export Control Office and the IT Department.

- Keep export control items and electronic devices in your carry-on luggage.

- For additional information, visit Defend Your Data.

Remember: If you don't need it - don't take it with you!!