International Travel Data and Device Guideline

Background

The University of Cincinnati (UC) promotes expansion of its global presence and as a result faculty and staff are at times required to travel internationally on behalf of the university. Information security and export control challenges are an ever-present concern for the university and the unique risks associated with international travel serve to magnify those challenges.

The disparity of laws of individual nations in conjunction with inherent border crossings involved in international travel may render typical security controls used to protect sensitive university data unworkable. For instance, encryption software as well as encrypted devices maybe subject to legal restrictions in some jurisdictions. Foreign governments sometimes monitor, intercept and record communications and in addition may upload malware or viruses onto mobile devices in covert operations. Laptops, tablets and mobile devices may be subject to search and seizure by U.S. Customs and Border Protection, as well as other national law enforcement entities, without probable cause of suspicion, a reality that requires the international traveler seriously consider what information is absolutely necessary for overseas travel. To assist university faculty and staff the Office of Information Security (OIS) offers this guideline detailing precautions to be taken and measures to be employed to protect sensitive university data, devices and intellectual property during international travel.

Prior to departing

- In preparation for international travel on official university business the prospective international traveler may want to consider contacting their unit IT and/or OIS to discuss data security and compliance considerations during international travel.

- Check to see if the destination country has any encryption use or import

restrictions. For example, China, Israel and Russia have restrictions on encryption tools use and import. If encryption tools are restricted and there is no personal use exemption, the use of a clean loaner device is strongly recommended. Contact unit IT and/or OIS about availability of existing devices for travel.

- If a loaner device is not used, the laptop should be backed up and unnecessary files and applications should be removed leaving only files and applications of absolute necessity on the laptop. It is also recommended this be done for any applicable mobile device taken.

- All applications should be fully updated and securely patched.

- All file-sharing and print-sharing services should be turned off.

- Only data of absolute necessity should be on any device(s) in the traveler's possession.

During International Travel

- Never leave the laptop, tablet or other device(s) unattended and always utilize encryption when permissible.

- Turn off Bluetooth, RFID, NFC and other wireless services except when necessary and being used.

- The physical security of the device(s) should of concern at all times and the traveler will be required to employ sound judgment in determining the most secure location for the device(s) keeping in mind that typical storage solutions (e.g. hotel safes) could, under international travel conditions, result in unreliable means of secure storage. All technology assets should be in the traveler's immediate possession at all times.

- Do not store sensitive university or personal data on any internal or external local media.

- Sensitive university data should remain stored securely on university servers and accessed remotely using secure VPN services.

- Do not use hotel or other Wi-Fi access points to receive or transmit data as they are notorious for data theft and interception.
- Use private browsing features in web browsers.

- Be cautious in using GPS related applications.

- Do not save usernames or passwords in the browser or any other application.

- Utilize physical locking devices when additional protection is needed.

- Turn off wireless services when not in use or when network connectivity is not required. Any connectivity credentials created or used while traveling must be noted and changed upon return. Do not use the same password for multiple services as that my lead to compromise.

- Do not use an Administrator account as your primary user account.

Upon Return from Travel

- If a loaner device was obtained from unit IT or OIS do not connect to the university network or home network before returning the loaner device. The device must be properly sanitized by your unit IT and/or OIS.

- If a loaner device was not utilized, re-install files and applications from the previous back-up. Under ideal conditions a drive format and re-installation of the operating system should be undertaken as a countermeasure to more insidious activity such as a covert installation of a rootkit.

- Change all passwords that were used during travel.
- Change all credentials that were used to access any services.