International Travel Data Security Procedure

Executive Summary Contact: Henry Torres, (870) 972-3033

Background:

- The Security Task Force recognizes the importance of maintaining the integrity and security of ASU technology assets. International travel poses a myriad of risks with respect to technology assets including data loss and system compromise and as such exposes the University to liability.

Summary:

- Employees will not be allowed to take personally assigned ASU equipment on international trips.
- Upon employee request to his/her direct supervisor, ASU will provide a "loaner laptop" system on which is loaded only the information necessary for that particular trip.
- The loaner laptop will be equipped with whole disk encryption software.
- As smartphones are subject to the same search and seizure guidelines and security risks, travelers will be provided with a "loaner phone."
- International travelers should notify ITS 30 days in advance of their departure and anticipated return date to ensure availability of loaner devices. Upon return, the loaner device must be returned to ITS within 7 days for a complete rebuild. In the event that the device is lost or stolen, ITS should be notified immediately.
- The loaner device SHOULD NOT be connected to your home network nor the ASU network prior to returning it to ITS due the risk of malware.

Consequences:

- Failure to comply with federal export regulations can result in substantial fines to the University
- Failure to comply with federal export regulations can result in substantial penalties including imprisonment

International Travel Data Security Procedure

As ASU continues to expand its global presence, faculty and staff are often called upon to travel internationally to support these efforts. As with any travel, there are certain basic things that all employees can do to help keep technology assets and sensitive information secure. International travel however presents its own challenges with respect to information security and should be addressed accordingly.

International Destinations

University travelers should be extremely vigilant when traveling with their personal laptops, tablets or other communication devices such as smartphones. Many foreign countries monitor, intercept and record electronic communications as well as introduce viruses, Trojans and other malware onto mobile devices without the traveler's knowledge. In light of this potential, there are certain basic things that a traveler can do in order to minimize the risk associated with unintended data loss or theft.

These precautions include:

- Never leave your laptop, tablet or your smart phone unattended. This includes never locking your device in your hotel safe. It is well know that in-room safes can be accessed by hotel staff with the end result being access to your technology devices by unknown actors. The same applies for hotel lockboxes and hotel safes in the lobby. These also can be accessed at any time by hotel personnel or by foreign intelligence operators and provide no security for your technology devices.
- If you must take a laptop when traveling, always use encryption to protect sensitive files and perform regular backups to ensure that you suffer no loss of vital information in case of theft.
- Do not use hotel Wi-Fi or other Wi-Fi access points to receive or transmit data. These Wi-Fi points are notorious for data theft and present an easy avenue for malicious actors to intercept your data and/or other transmissions.

The best course of action is to take as little sensitive information as possible when traveling overseas. As stated previously, all technology assets should remain in your possession at all times. This includes any other types of media such as flash drives or other computer disks.

At the U.S. Border

While information security is usually a top concern when traveling overseas, it is worth noting that data loss can occur at the U.S. border. The agencies of the Department of Homeland Security have the right to search and seize laptops and other electronic devices at the nation's border.

Under the agency directives for the Immigration and Customs Enforcement Agency, searches are allowed absent any individualized suspicion and agents can confiscate a digital device for up to 30 days without any supervisory approval. Under Customs and Border Protective guidelines, agents can keep a device for up to five days without any further approvals.

Given that laptops or other digital devices are subject to search and seizure at the U.S. border without probable cause of suspicion, it is prudent that travelers carefully think about what information is absolutely necessary for their overseas travel.

In light of the above, ASU has adopted the following procedures for international travelers:

- Employees will not be allowed to take personally assigned ASU equipment on international trips.
- Upon employee request to his/her direct supervisor, ASU will provide a “loaner laptop” system on which is loaded only the information necessary for that particular trip.
- The loaner laptop will be equipped with whole disk encryption software.
- As smartphones are subject to the same search and seizure guidelines and security risks, travelers will be provided with a “loaner phone.”
- International travelers should notify ITS 30 days in advance of their departure and anticipated return date to ensure availability of loaner devices. Upon return, the loaner device must be returned to ITS within 7 days for a complete rebuild. In the event that the device is lost or stolen, ITS should be notified immediately.
- The loaner device SHOULD NOT be connected to your home network nor the ASU network prior to returning it to ITS due the risk of malware.

International travelers taking any software out of the United States that is not covered under the safe harbor rule of “publicly available” should consult Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR) for further guidance.