Arkansas State University
International Travel Data Security

As A-State 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. However, international travel 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. To mitigate these risks, travelers should take these basic steps to deter unintended data loss or theft:

- Never leave your laptop, tablet or your smartphone unattended. This includes never locking your device in your hotel safe. It is well known 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, so they 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, 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, A-State has adopted the following procedures for international travelers:

- Review and follow International Travel with Institutional Devices Guidelines. This is a tiered system based on institutional and individual risk and traveler need.

- A-State ITS can provide a “loaner laptop” system on which is loaded only the information necessary for that particular trip.

- As smartphones are subject to the same search and seizure guidelines and security risks, please complete the BAG and/or TMP, as appropriate. Also, please notify the Director of Research Compliance (export@astate.edu) if you intend to carry an A-State assigned cell phone abroad.

- 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 with 7 days for a complete rebuild. In the event that the device is lost or stolen, ITS should be notified immediately (security@astate.edu).

- The loaner device SHOULD NOT be connected to your home network nor to the A-State network prior to returning it to ITS due the risk of malware.

Arkansas State University - Jonesboro

ITS Equipment Check-Out Form

Name: ______________________ Equipment pickup date: __________

Destination countries: ______________________ Equipment return date: __________

Department: ______________________ ID number: __________

ITS is prepared to offer a limited number of "clean" laptops to faculty and staff traveling internationally on A-State business. Please note that requests will be filled based on availability.

I request the following equipment for travel abroad: ☐ **Laptop** ☐ **Tablet**

Has the equipment been reserved at least 30 days prior to my travel date, to allow time configure the device in accordance with export controls guidelines?	☐ Yes	☐ No
Will any additional software be installed on any device that may require additional licensing? If so, this process will need to be handled through the Office of Research Compliance.	☐ Yes	☐ No
I understand that I should not connect to the A-State network via a VPN or via MyCampus at cybercafés or public kiosks or shared computers, because these locations might contain keylogging software that could steal my identity credentials.	☐ Yes	☐ No
I agree that USB, flash drives, and any other device that transmit information should not be connected to A-State resources upon my return or until ITS has scanned for viruses and given clearance to use.	☐ Yes	☐ No
I agree to access my work related e-mail only through the loaner laptop via the AState website link to the Faculty/Staff webmail or through the MyCampus portal. I will not use the Outlook software application that is on my laptop computer. I agree to only access Blackboard and Banner through the MyCampus portal.	☐ Yes	☐ No

______________________________ __________

Signature Date

For questions regarding software, technology, data security, or export control, please contact:

A-State ITS (870) 972-3033, or
Director of Research Compliance (870) 972-2694.