SIU

Southern Illinois University System

International Travel Tips for High-Risk Countries

Business travel to China, Russia and other high-risk countries, whether for research, clinical or consulting purposes, creates specific information security challenges that must be addressed in order to effectively secure SIU's data and assets. The SIU Clean Laptop Program has been put in place to address these concerns. The below tips provide further guidance for travel to high-risk countries.

Travel Statement

All SIU workforce members traveling to high-risk countries must take special care to ensure SIU's data and assets are properly secured, due to the fact that personal privacy may not be respected. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio, or other monitoring. Workforce members are advised to assume that anything done on any device, particularly over the Internet, may be intercepted. In some cases, encrypted data may be decrypted.

Prior to Travel

- Review the high-risk countries list. If your travel destination appears on the list, you must follow the procedures in the SIU Clean Laptop Program.
- Consider the Travel to High-Risk Areas guidance provided by the U.S. Department of State.
- Change all passwords prior to departure.
- Backup your laptop and/or phone before departure.
- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, employee badge or fobs you would use to access your workplace, or other areas, and any other access control devices you may have at home.
- Remove any financial information such as bank account numbers, logins and passwords you may have in your purse or wallet.
- Document the account numbers to anything you do take, so that if lost/stolen, you know what is missing.
- Obtain and use an RF-shielded cover or case for any RFID cards (including U.S. Government Nexus "trusted traveler" cards) that you do plan to take with you.

During Travel

- **Never use** shared computers in cyber cafes, public areas, hotel business centers, and never use devices belonging to other travelers, colleagues, or friends.
- Rigorously apply minimum necessary principles to all information accessed, used or obtained.
- When not in use, completely logout of applications accessed and fully power down devices. Do not allow them to be in “sleep” or “hibernation” mode, make sure they are shutdown.
- Keep device(s) with you at all times during your travel. Do **not** assume they will be safe in your hotel room or in a hotel safe.
- Do not send sensitive messages.
- Disable and fully cover any integrated laptop cameras.
- Physically disconnect any integrated laptop microphones.
- Be aware of your surroundings and shoulder surfing. Position yourself to minimize this opportunity for others.
- Disable all unnecessary network protocols, (e.g., Wi-Fi, Bluetooth, infrared, location services, GPS, etc.)
- Do not plug your phone into charger kiosks. There may be a hostile computer on the other end of that innocent-looking wire.
- Access to services that we take for granted like Gmail and other Google apps, Wikipedia, and Yahoo Web Mail are often blocked altogether or monitored/filtered.
- Do not store any sensitive data on your devices while traveling overseas.
- Do not use or borrow others' USB memory sticks.

Upon Return to United States

- Immediately discontinue use of the travel laptop you brought with you.
- Change all passwords you may have used abroad from an alternate device (other SIU/Institution workstation/Laptop).
- Do not plug in any USB memory sticks that you have obtained/received during travel.
- Return the travel laptop following the instructions for your campus in the SIU Clean Laptop Program.