Office of the Vice President for Research
Iowa State University

Unit: Office of Research Integrity
Effective: Immediately
Reviewed/Revised:
Contact: vpr@iastate.edu

International Travel and Information Technology: Helpful Tips Before, During, and After
Guidelines

Pre-Travel

- **Passwords**: Passwords should be complex and non-repeating; don't use the same password for multiple accounts.
- **Take a loaner**: If possible, take a clean, blank device. Leave all unnecessary devices at home. Mobile phones should also be clean because contacts lists can be gathered and used for fraud/phishing scams. Most smart phones have a SIM card that can be stolen just as easily as a computer (and often contains password data in the cache).
- **Email**: If possible, set up a temporary email account for your travels. Email/passwords can be used to recover usernames and passwords on a number of sites and systems.
- **Data reduction**: Store all data on a flash drive that you carry on your person. Do you have sensitive information on your hard drive that is not necessary for your trip? If so, transfer it to an external drive and leave it at home.
- **Sponsored data**: All data and software that are specifically designed or modified for military/space use are forbidden to be taken out of the United States. Additionally, do not travel with data sponsored by a non-disclosure agreement.
- **Investigate your destination**: Know the security and safety concerns for your destination. Visit the U.S. State Department (www.state.gov/travel) to learn the most up-to-date information.
- **Equipment**: DO NOT take Iowa State or sponsor-loaned equipment (unless it is a clean, loaned device) outside of the country unless it is critical for your research.

During Your Stay

- **Monitoring**: Assume your devices are compromised and being actively monitored.
- **Privacy**: Do not expect that your privacy will be the same as it is in the U.S. and Canada. Your room and personal items can be accessed or seized without your consent or knowledge in certain countries.
- **Turn off mobile connections**: If you do not need access to the internet, turn off wireless connections in your devices. Non-networked devices are much harder to break into remotely.
- **Keep it with you**: If you have sensitive data or mobile devices, refrain from leaving them in your room.
- **NO ACCESS**: DO NOT access secure servers/databases that contain sensitive or export-controlled information. Treat every keystroke you make as being recorded.

Post–Travel

- **Quarantine**: Refrain from connecting your device to a network until you've had IT thoroughly inspect the device for malware and viruses. Some malware does not activate until it connects to a home network.
- **Passwords**: Change every password for sites and systems you accessed while traveling internationally.

Unit: Office of Research Integrity
Effective: Immediately
Reviewed/Revised:
Contact: vpr@iastate.edu

Contact

Office of Research Integrity
2420 Lincoln Way, Ste. 202
Ames, Iowa 50014
export@iastate.edu