Information Security Guidelines for International Travel

Function: Information Security
Procedure: Information Security Procedure for International Travel
Contact: Chief Information Security Officer

Guideline Recommendations

Individuals who travel internationally with laptops, phones, and other mobile devices are at risk of theft, seizure, or loss of these devices, as well as potential compromise from cyber intrusion or malware. In addition, Research Foundation for SUNY ("RF") employees and representatives may possess or have access to information that is highly sought after by foreign entities, including: proprietary intellectual property; research, development, testing, and evaluation; program milestones and specifications; and system capabilities. Foreign entities also may target information related to the RF's personnel, security, and operations.

You are the first line of defense in protecting confidential and proprietary information. The following guidelines cover Safe Computing Tips, Confidential Information, and Export Control information you should be aware of when traveling internationally.

Safe Computing Tips

- Ensure your device(s) are patched and have up to date anti-malware software enabled.
- Ensure multi-factor authentication (MFA) is utilized for all account access wherever possible.
- Don't use "public" computers to conduct business. For example, don't use commonly accessible computers at internet cafes, hotel business centers, etc.
- Don't use "public chargers" at airports. These can be a direct data connection into the device and can allow malicious actors to steal the data from your device.
- Don't plug in foreign (unknown) portable storage devices such as USB flash drives, or portable hard drives, even if they are giveaways at conferences or meetings you attend.
- Use Virtual Private Networking (VPN) software to connect to systems containing sensitive data whenever possible.

- Be aware of event-related targeted emails if you are traveling for business purposes. You may be tempted to let your guard down when opening email dealing with your planned business events but remember these may be publicly known and are a prime target for phishing campaigns.

- Turn on "airplane mode" whenever you don't need to be connected to the internet. It's an easy way to minimize the opportunity for hackers to break into your device over your Wi-Fi or Bluetooth connection.

- Remote locate/wipe capabilities should be enabled on devices whenever possible in case of loss/theft.

- Have the contact information of your Tech Support Help Desk along with incident reporting procedures with you while traveling.

- Remember that device confiscation at borders is possible. Don't bring anything you aren't prepared to lose.

Confidential Information

Travelers must not transport confidential information outside the US on any computer system or storage device such as laptops, tablets, cell phones, USB drives, SD cards, etc., even if the device employs data encryption. Examples of confidential information include but are not limited to:

- Controlled Unclassified Information (CUI)

- Covered Defense Information (CDI)

- Personally Identifiable Information (PII)

- Protected Health Information (PHI)

- Confidential research data (including any information that is defined as confidential information in sponsored awards, non-disclosure or other agreements)

Travelers must not access confidential information remotely from outside the US.

Export Controls

U.S. export control and sanctions programs may affect your foreign travel. Technical data including encryption technology, e-documents, drawings and software may be controlled under US regulations and require permission to take to another country. This includes data on laptops and other smart devices that remain in your possession. While many of these items can be temporarily exported under the EAR license exception "Temporary exports -Tools of the Trade" (TMP) or Baggage (BAG), this needs to be confirmed and it is the responsibility of the traveler to ensure they are complying with the regulations. Violations can lead to civil or criminal penalties and seizure of the devices. Visit the Export Control Exclusions and Exceptions page at the RF website for more details: Exclusion Exceptions (rfsuny.org).
There may be additional export restrictions imposed by sponsors. Travelers should contact their appropriate campus Sponsored Programs office to assure compliance with sponsor guidelines.

Change History

Date	Summary of Change
April 17, 2023	New Guideline.

Feedback
Was this document clear and easy to follow? Please send your feedback to webfeedback@rfsuny.org.