ISC Information Security
Best Practices for Data Security on Foreign Travel

There are many good general recommendations for staying safe while traveling. This document is specifically designed to help you identify some key steps to take to protect ***Penn systems and data*** while abroad, and is intended to complement the information contained on Penn's Global Support Services website: http://global.upenn.edu/gss:

Before You Go

- Information technology support is provided at Penn through Local Support Providers (LSP's), who provide support services and options for the various Penn constituencies (e.g., faculty, staff, student). Contact your LSP in advance of your travel and work with them to identify options for computer repair and service. If you are not sure who your LSP is, please visit www.upenn.edu/computing/view/support/ for details.
- Work with your LSP to conduct a full backup your system and all its data and to ensure all software is up to date and appropriate security tools (such as disk/device encryption, password locking, location services, and remote wiping) are functional.
- Work with your LSP to enroll in Penn's Two Factor service for PennKey:
    - http://www.upenn.edu/computing/weblogin/two-step/. (Make sure to print out sufficient single-use codes in case your phone is lost or stolen).
- Avoid taking any sensitive or confidential university data (e.g., sensitive Personally Identifiable Information, proprietary information, or data whose disclosure would cause significant harm to Penn or its constituents) unless absolutely necessary.
    - If you are not working with your LSP to regularly scan your systems for unneeded sensitive data, you should begin doing so now.
- Encrypt data if it is essential that you take it with you.
    - **Note:** Users intending to travel to Cuba, Libya, North Korea, Syria, Sudan, Iran or Iraq should contact the Office of Research Services for assistance before exporting Penn owned equipment or data. (Additional information below).
    - Certain countries may inspect laptops and data upon entry, so you should be careful about proprietary, patentable, or sensitive information that may be stored on your device. If you have encrypted files, customs officials in some countries (including the U.S.) may require you to decrypt the files for inspection. ***In short, be prepared when traveling abroad that you may be compelled to share any data brought with you.***
    - Ask your LSP if a sanitized "loaner" computer is available to help avoid unnecessarily exposing all your data to known and/or clandestine inspection.

While You're Away

- Not all WiFi connections are equal. WiFi connections that encrypt traffic, are restricted with a password, and provided by a trusted source (University, colleague, hotel, etc.) are preferable to free and/or unencrypted services. Know your wireless networks and use encrypted services whenever in doubt (e.g., HTTP**S** over HTTP when web-browsing).
    - If you must use a free WiFi connection, avoid connecting to any website or service that requires password authentication and is not securely protected (including Penn systems with sensitive data, banking and other financial sites, etc.).
- Similarly, avoid accessing sensitive websites from public computers, such as at Internet cafes, as their security is highly unreliable.

- If possible, do not insert USB ("thumb") drives or other portable media given to you when traveling. If it is necessary, make sure your virus definitions are up-to-date and scan any inserted media for malware.
- An ideal solution may be to run a VPN-client (Virtual Private Network), to allow you to securely and directly access Penn's network from abroad. Talk to your LSP for more details.
- **Note:** If you have secure and reliable Internet services overseas, it may be more cost effective to leverage services hosted at Penn (e.g., webmail, Penn+Box, etc.).
- Be vigilant with mobile devices. Keep them on your person or in a locked safe whenever possible. If your device is stolen, notify your LSP immediately. Enable a PIN, remote wiping and other key security features as recommended in *Penn's Top 10 Security Tips for Smartphones & Tablets* (http://www.upenn.edu/computing/security/checklists/Top10/).

When You Return

- Work with your LSP to securely transfer any new data, restore any removed data and scan your system for malware.
    - In some instances (e.g., after connecting to insecure networks, after visiting certain countries deemed sensitive) it may make sense to wipe and reinstall the operating system as a precautionary countermeasure against unseen tampering or infection.
- If used while on your trip, this is a good time to consider changing your PennKey password as well: http://www.upenn.edu/computing/pennkey/setreset/

A special note about Privacy

Be sensitive to local privacy laws as well. Contact the Office of Audit, Compliance and Privacy (privacy@upenn.edu) for advice regarding the applicability of international privacy regulations if you will be working with other people's personal information. (This is particularly true if you are working in EU Member Countries or Argentina, Australia, Hong Kong, Sweden and Canada).

Export Control Compliance

Please note that some software and data may be subject to Export Control Regulations. Simply accessing export controlled data while outside the U.S. (e.g. opening files on a Penn server accessed via a VPN connection) may be an export of that information subject to the regulations. For questions related to International Trafficking in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) compliance, please contact the Office of Research Services (http://www.upenn.edu/researchservices/exportcontrols.html).

External Links & Resources:

- U.S. Department of State International Travel Advisories: http://travel.state.gov/travel/travel_1744.html
- Federal Bureau of Investigation: Safety & Security Abroad for Professionals & US Students http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure http://www.fbi.gov/about-us/investigate/counterintelligence/student-travel-brochure-pdf
- Traveling Light in a Time of Digital Thievery (New York Times, 2/10/12) http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=2
- Department of Commerce – Travel considerations: http://www.bis.doc.gov/policiesandregulations/regionalconsiderations.htm

For more information and resources please see the Information Security website at http://www.upenn.edu/computing/security, or contact us at security@isc.upenn.edu or 215-898-2172.