Carnegie Mellon
INFORMATION SECURITY OFFICE

International Travel Guidance

Last Updated: July 20, 2016

This guide is primarily intended for CMU faculty, staff and students traveling outside of the United States on behalf of CMU. Much of this information also applies to traveling outside of the United States for personal reasons as well. **If you have a US security clearance, please contact your security officer for further requirements that will apply to you.**

Preparing for Your Trip

Before you leave, there are several things you should do in preparation for your trip.

Review Department of State country information for the countries you are traveling to

https://travel.state.gov/content/passports/en/country.html

The Department of State maintains country specific information on every country in the world. It provides information about whether you might need a visa (if you are an American citizen), crime and medical considerations, and laws that might be significantly different than in the US. It's a great source of information, especially if you have never traveled to that country previously.

Obtain visas and vaccinations as required

Allow enough time for processing if the country you are traveling to requires a visa, or requires specific vaccinations

Review Office of Research Integrity and Compliance (ORIC)'s notices

http://www.cmu.edu/research-compliance/export-controls/foreign-travel.html

ORIC maintains export compliance for the University. They can help you navigate specific situations involving export of information such as research. They can also tell you if you will be unable to encrypt your data while traveling. If you are traveling to an "at risk" country (defined by the Office of Foreign Assets Control at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx), **always** contact ORIC before you travel.

Consider taking alternate computing devices

Consider not taking your usual work or personal laptop, tablet or phone. Do you really need it? Your devices and data will be safest if they remain at home or in a locked office on campus. Check with your department IT staff if there are loaner laptops available for you to use. These laptops should have basic tools installed, but none of your sensitive data and no software that is subject to export control. Remember, even as a US citizen, US customs can seize your devices at US borders, not to mention any other country's customs.

Purchase the correct power adapters, plugs, and transformers for your devices

Most countries do not use the US style plug or voltage, and you will still need to charge your devices. Research the plug or plugs and any transformers you will need prior to traveling (http://www.worldstandards.eu/electricity/plugs-and-sockets/). Most laptops do not require a transformer, but check your manufacturer's manual. Don't forget to bring a way to charge your cell phone, iPod, camera, etc as well!

Enable Full Disk Encryption for all of your devices

If you do choose to take your laptop, enable full disk encryption if you are able – see http://www.cryptolaw.org/ for countries where encryption is not permitted (somewhat outdated). An encrypted disk prevents anyone from having easy access to your data if they physically steal your laptop.

Native encryption is available in OSX as "Filevault" and in Windows as "Bitlocker" (Windows 8 or above). Linux, especially Ubuntu, has LUKS – Linux Unified Key Setup.

Run Identity Finder

Especially if you are unable to encrypt your laptop, run identity finder on it to make sure that you do not have any personally identifiable information on it (http://www.cmu.edu/computing/security/idfinder/index.html).

Secure Your Computer

Follow the instructions available at http://www.cmu.edu/computing/security/start/index.html to secure your computer. This involves things such as updating your system, installing anti-virus, setting a password, and turning on the firewall. These general security tips will help you both while traveling and at home.

Turn off file and print sharing

Disable remote access to your computer. Instructions can be found at http://www.cmu.edu/computing/security/fileshare/

Download the CMU VPN software

http://www.cmu.edu/computing/network/vpn/index.html
Make sure you have the CMU VPN software on your laptop. This allows you to create a secure connection to campus for use of campus resources. The default VPN will **not** encrypt all of your traffic, just traffic to campus IP addresses. If you would like to encrypt all traffic, use the Library Resources VPN (http://www.cmu.edu/computing/network/vpn/anyconnect/client/create.html). You will experience degraded performance, but all traffic from your laptop will be encrypted to campus prior to being routed to its final destination.

Backup your devices

Backup your devices regularly and especially before you travel, including laptops and mobile phones. If either one is stolen, you will have a backup for restoration of your data.

Enable a password and automatic wipe of mobile devices

Configure your mobile device to require a password and enable a data wipe after 10 failed attempts. Exchange customers can do this through MyExchange Tools https://myexchangetools.cmu.edu/manage-mobile.aspx. Select **CMU Secure Policy II** from **Manage Mobile Policy**. Look at your device's manual for how to do so if you do not use Exchange. Verify that you have a good backup of your device to recover from in the event that you need it.

While Traveling

DO NOT leave your device unattended

Keep your device with you at all times. If your hotel room does not have a safe or you are staying in alternate accommodations, bring a lock with you to secure your computer in your room while you are away (such as at a meal).

DO NOT plug in untrusted accessories

Do not plug in untrusted accessories such as a flash drive, or charging cable (for mobile phones). If you need to purchase an accessory while traveling, purchase from a reputable source.

DO NOT use public kiosks

Public kiosks, like those at hotels, are often loaded with malware and key loggers that will capture your username and password. If you do use one (such as for printing out a boarding pass), change the password for the account you used as soon as you can access a secured computer.

Connect only to known wireless networks

Attackers commonly set up "Free Wifi" access points to encourage unsuspecting people to connect and then harvest credentials. Make sure that you are using the provided public wifi in an area, check with the staff at your hotel or other business for the correct network to join, and use only that one.

CMU is a member of eduroam, the network of university wifi networks, and if you are near a university, you can connect to their wifi for free using your @andrew.cmu.edu credentials. This network would appear as "eduroam" on your available wifi networks.

Use the Campus or Library Resource VPN

Using CMU's VPN software, you can connect securely to campus resources and other resources off campus (via the library VPN).

Follow safe computing practices

Be cautious about links you click on, software you download, etc. More information about general safe computing can be found on the ISO's web pages at

http://www.cmu.edu/iso/aware/secure/index.html and
http://www.cmu.edu/iso/aware/be-aware/index.html

Notify the Information Security Office if concerns arise while traveling

If you suspect unauthorized access of your device(s) or accounts, notify the Information Security Office as soon as possible.

When you Return

Reset/Change the password for accounts you used

This is especially important if you used them at public kiosks or on untrusted computers. Changing your passwords ensures that even if someone did gain access to your credentials while you were traveling despite the precautions you took, they will be unable to use them. Make sure you use a secure and trusted computer to change your passwords. Do not choose previously used passwords. Do not choose passwords used for other accounts.

Notify the Information Security Office if concerns arise following travel

If you suspect unauthorized access of your device(s) or accounts or observe anything suspicious related to device behavior or email after your return, notify the Information Security Office as soon as possible.

Revision History

Version	Date	Author	Description
1.0	20-JUL-2016	Laura Raderman <lbowser>	Initial Document