23. International Travel Standard

When traveling internationally, you may be subjected to more security risk than usual. This applies to both your personal devices and information as well as CMU data and equipment. When travelling internationally, be sure to plan ahead so that you understand these risks and how to best mitigate them. Engage this process early, as some of the approvals and required steps require advanced notice and preparation time.

Purpose:

This standard provides recommendations for the responsible use and proper stewardship of the University's technologies and electronic data when travelling internationally. These recommendations are derived from industry standard information security practices, and they support and conform to federal travel warnings, restrictions, and export control regulations.

Quick Reference:

1) **Personal international travel.** If you plan to take a computer and/or phone with you, make sure you have backups of your data prior to leaving the country. Be sure to add security protections such as a strong password and disk encryption to keep someone else from being able to access the device or data in case of loss or theft. In addition, review the rest of this document for further tips and considerations.

   Important: If you are traveling with university devices or data, you are required to protect them against theft, loss, and exposure at all times. Any security incidents must be reported as soon as possible. All of the requirements and advice in this document apply to university devices and equipment wherever they are.

2) **Are you traveling for work- or professional-related activities?** If so, you must:
   a. Receive formal permission/approval for international travel from University Administration
   b. Review and decide if you are travelling to a "high risk" risk country
      i. "High risk" countries may be subject to export control regulations
      ii. "High risk" countries may require you to add many extra security precautions, or require you to get a loaner laptop and loaner cell phone, or not take one with you at all. You may also need to do things before you go and after you return to keep University data and your personal data safe.
      iii. "High risk" countries may also be physically dangerous for you to visit.
   c. Be aware that all travel increases likelihood of loss of devices and/or exposure of data.
   d. Review this document for computer and data-related considerations of:
      i. How to get ready for travel
      ii. How to travel light
      iii. How to keep your devices safe
      iv. How to keep your accounts from being compromised
      v. What to do if something goes wrong
      vi. What to do after you return
3) Some "loaner" laptops are available through the Park Library. These laptops are configured specifically for security during international travel.
4) Cell phones and mobile hotspots are available for short-term rental through CMU Connect in Woldt (certain restrictions, conditions, and charges may apply).
5) All computer and data-related travel considerations should be coordinated through your technical support personnel. Please submit a ticket through the OIT Help Desk to schedule a review with your local technicians.
6) Most travel is not "high risk" and is no more dangerous than traveling locally or within the U.S., but international borders and other laws can come into play, so make sure you know what applies to you.

International travel can pose potential, significant risks to information stored on or accessible through computers, tablets and smartphones, and access to credentials and information accessed while travelling. Some of the risk is associated with increased opportunities for the loss or theft of the device due to the distractions of traveling. Connecting to and transmitting information over networks or devices owned or managed by foreign or unknown and untrusted entities also introduces risks not present under normal, non-travelling circumstances (for instance, opportunities for digital eavesdropping, data capture, malicious code injection or infection, connection hijacking, and broadcast over unencrypted (non-private) wireless connections).

Additionally, many information security regulations require information be kept secure and confidential while travelling or in transit, and export control regulations prohibit the transport and transfer of technologies and information to some countries and their citizens. Choosing what information and technologies to take, and how to protect them, is the traveler's responsibility. This standard is intended to help guide and protect them.

Scope:
This standard applies to all University-owned systems, devices, and electronic information, and as noted in the Responsible Use of Computing Policy, to all systems and devices accessing University systems and Institutional Data. Individual travelers are responsible for knowing the regulations applying to them and the devices and information they transport, access, use, and transfer.

Standard:
International Travel and Export Control Standard

Travelers are responsible for knowing the applicable regulations and requirements, and applying these recommendations to their travel plans and situations:

1. **Assumptions while traveling:**
    - **No device can be protected against all** possible forms of system and information compromise, especially when its members travel to countries that are deemed as high risk. We should assume that any device taken to a high risk country will be compromised in some, potentially undetectable way. The only truly secure option is to refrain from using digital devices when traveling.
    - **Information of particular interest** to someone intent on compromising your devices not only includes personal and University data, but also the traveler's Global ID and password which can be used to directly access University systems and information resources.
    - **When a device is compromised**, the attacker may install software on the device that could compromise other systems and data on the University's network. Upon return, measures must be taken to completely restore the device to its pristine or pre-travel state before the traveler reconnects his or her device to our network. This requires a backup of the device prior to travel, or use of a loaner device instead.
    - **Consider taking no devices or using loaners instead.** OIT has loaner devices available to use, and in some cases (for instance, cellular phones in high risk countries), you may be better off using no devices or purchasing new devices for use while there.

2. **Preparing for your trip:**
    - **Identify the risk levels of the countries you plan to visit:**
        - "High Risk"
        - Non "High Risk" (Moderate, Low, etc.)

      Refer to the U.S. State Department's "Travel To High Risk Areas" web page for travel advice and to identify "high risk" countries, and for travel warnings for countries you plan to visit. See: https://travel.state.gov/content/passports/en/go/TraveltoHighRiskAreas.html

      Review the U.S. Department of Treasury Sanctions web site for any applicable country sanctions:

https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

Review the CMU ORGS export controls site resources on CentralLink:
https://www.cmich.edu/office_provost/ORGS/ComplianceandResearchIntegrity/Export%20Controls/Pages/default.aspx

- **Understand the sensitivity of any data you plan to bring or access:**
  Review what you're planning to take with you and access while travelling, and seek ways to limit the amount of sensitive information that you take on your trip. Take only what's necessary.

  > Removing unnecessary confidential data from any device reduces the risk of exposure to anyone gaining access to the information. Examples of data that should be left on campus or afforded exceptional protection include information that might be considered sensitive by the host government, is governed by a Data Use Agreement, contract, or other formal arrangement stipulating that it may not be transported to planned travel destinations, and information defined as Restricted or highly Restricted by the University's Data Classification Standard (for instance, HIPAA data, FERPA data, and student and employee PII).

  As part of travel, you may be required or asked to power-up and login or unlock electronic devices for review by travel control officials. This may represent a breach of confidentiality of the information, and thus if the data isn't needed during the period of travels, it should not be taken along on the device (or if needed, should be additionally protected with strong encryption and separate passwords on the device).

3. **Implement recommendations or protections required for travel to those countries:**
   - **Travel to High Risk Countries** requires special consideration and preparation. Planning ahead will protect your privacy and the University's data, and save a lot of money and frustration later. It's important to take the minimum you need in order to get your work done while you're gone. There are a range of options starting with the most secure and going down the minimum required actions.

   - **<u>Computers</u>**
   - **Best:** Travel light
     - We strongly recommend that you leave your current devices here and travel with a University-provided OIT Travel Loaner Device or kit. Use the Travel Loaner Device instead of your laptop; it will allow you to manage email, view your calendar, run presentations, edit documents, and connect to university websites. The devices are set up specifically for your use and wiped back to factory settings when you return. The Travel Loaner Device will provide you with a secure platform for the duration of your travel.
   - **Good:** Travel with less data
     - If you don't feel that you can travel without a full laptop, another option is to take a new or freshly rebuilt machine and load only the data you'll need for this trip. You'll need to make sure that the machine is encrypted before you go. Consult with your tech support personnel for assistance. Whenever possible, leave USB drives at home. These are easily lost and easily corrupted. If you must travel with a USB device, be sure that it's encrypted.
   - **Minimum:** Travel encrypted
     - If you can't travel with an iPad or a new computer and must take your own laptop, there are some additional steps you need to take before you go:
       - Verify that your computer software is current and fully patched
       - Make sure your computer is fully backed up and encrypted.
       - Remove any documents containing sensitive data from your computer.

    - When you return, save the documents you created while traveling to another device, completely wipe your computer, and restore it from the backup made before your travel.

- **A note about hotel safes:**
  Hotel staff and government officials in some countries can access hotel room safes, so don't expect that a computer or mobile device left in a hotel safe will be entirely secure from access or theft while you're gone.

- **<u>Mobile phones</u>**
- **Best:** Go without
  - The first thing to consider is whether you really need a mobile phone. Are you going to make calls? Can you get by with a Wi-Fi-only device like an iPad travel kit? Can you get by without a phone for a short trip? We're really tied to our phones these days, but perhaps you can go without.
- **Good:** Get it there
  - The best thing to do is to use a device you don't need to use again. This can be a loaner phone borrowed in the country, an unlocked phone with a local SIM card, or a phone you buy or rent at the airport or hotel when you arrive.
- **Minimum**: Use a University Loaner phone or have a plan for yours
  - The University can provide loaner managed and secured phones for use while travelling. These include daily use charges billed to the traveler.
  - If you must use your own phone:
    - Back it up before you leave,
    - Secure it using a locking PIN that wipes all data after a number of unsuccessful attempts to unlock it and enroll it in a "lo-Jack" type find & disable service like Apple's Find-My-iPhone.
    - Enroll it in an international rate plan to avoid incurring exorbitant roaming charges, and
    - Save your data, reset to factory defaults, and restore your backup when you return.

- **Travel to Lower Risk Countries** still requires special consideration and preparation, although not necessarily to the same extent as to high risk countries (but review those guidelines first). It's still important to take only the minimum you need in order to get your work done while you're gone.

- **<u>Computers</u>**
- **If you are taking your laptop computer**, before you go you should:
  - Verify that your computer software is current.
  - Make sure your computer is fully backed up and encrypted.
  - Remove any other documents containing Moderate or High Risk data.

- **<u>Mobile phones</u>**
- **Consider a loaner phone borrowed in the country**, an unlocked phone with a local SIM card, or a phone you buy or rent at the airport or hotel when you arrive. If you must use your own phone:
  - Back it up before you leave,
  - Secure it using a locking PIN that wipes all data after a number of unsuccessful attempts to unlock it and enroll it in a "lo-Jack" type find & disable service like Apple's Find-My-iPhone.
  - Enroll it in an international rate plan to avoid incurring exorbitant roaming charges, and
  - Save your data, reset to factory defaults, and restore your backup when you return.

4. **Additional recommendations for high and lower risk travel**
    - **Before you go:**
        - Empty your voicemail box.
    - **While you're traveling:**
        - Do not plug your phone into charger kiosks. There may be a hostile computer on the other end of that innocent-looking wire. Use your own charger.
        - Be aware of your surroundings. Watch for those looking over your shoulder (including security cameras) or potential thieves.
        - Do not leave your devices unattended. Even hotel safes are not secure.
    - **When you return:**
        - Change your Global ID password.
        - If you checked your voicemail while traveling, change your voicemail passcode.
        - If you brought your computer, save any documents you created while traveling to an external drive and restore from your pre-departure backup. Scan the external drive for viruses or malware when reconnecting it.

5. **What to do if something gets lost or stolen:**

    Traveling can be fraught with a variety of distractions - going through airport security, finding your way around town, getting used to cultural norms, etc. Unfortunately, most instances when mobile computing devices are lost or stolen occur in the areas where the distractions are the greatest. Recognizing distracting situations and, when they occur, taking extra care to maintain your focus can prevent you from having to take the steps necessary to disable those devices and obtain replacements.

    In case a laptop or mobile device is lost or stolen, contact a member of your department's technology support team or the OIT Help Desk at (989) 774-3662.

6. **Additional traveler guidance and resources:**
    - Below is a set of URLs with additional guidance, including much of the advice in this document (if links have become outdated, use parts of the descriptions below as search terms):

    - The U.S. Department of State's Country Specific Information for Students website:
      https://travel.state.gov/content/studentsabroad/en/beforeyougo/csi.html
        - Allows a user to specify his or her destination country for which it provides information such as, the location of the U.S. embassy and any consular offices; whether you need a visa; crime and security information; health and medical conditions; drug penalties; and localized hot spots.

    - The FBI's Travel Tips brochure:
      https://www.fbi.gov/file-repository/business-travel-508.pdf/view
        - Measures that the FBI recommends taking before, during and after traveling internationally in a compact, printable document.

    - US CERT's Holiday Traveling with Personal Internet-Enabled Devices website:
      https://www.us-cert.gov/ncas/tips/ST11-001
        - Tips from the US Computer Emergency Readiness Team for protecting your mobile devices when traveling.
        -

    - Internet 2's Security Tips for Traveling Abroad website:
      https://spaces.internet2.edu/display/2014infosecurityguide/Security+Tips+for+Traveling+Abroad

- A collection of institutional, governmental and other resources that provide guidelines for secure, international travel.

Responsibility and Sanctions:
All users of University computing resources are responsible for security, proper data stewardship (handling of Institutional Data), and the protection of University computing resources.

Failure to comply with these information security standards may represent a violation of the Information Security policy, the Responsible Use of Computing policy, the Data Stewardship policy, and/or other applicable University policies. Violations of the Information Security Policy may result in suspension or loss of the violator's use privileges with respect to Institutional Data and CMU-owned Information Systems, and additional administrative sanctions may apply up to and including termination of employment or contractor status with CMU (civil, criminal and equitable remedies may also apply).

Frequently Asked Questions
Refer to the Information Security Standards FAQ for additional information regarding this standard.

References
Administrative Policies and Procedures Manual:
https://www.cmich.edu/office_president/general_counsel/Pages/policies.aspx
Responsible Use of Computing Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03031.pdf
Data Stewardship Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03030.pdf
Information Security Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03042.pdf
Computer Disposal Policy:
https://www.cmich.edu/office_president/general_counsel/Documents/p03012.pdf
About Information Security and the Office of Information Technology (OIT):
https://www.cmich.edu/office_provost/OIT/About/Pages/default.aspx

Additional Information
Questions or concerns related to this information security standard should be directed to CMU's CISO at 989.774.7445. Additional information can be found on the University web page at www.cmich.edu.

Document History
This is the third draft of this document. Last updated March 17, 2017