International Travel Guidelines

Purpose: International travel presents unique risks to personal and information security compared to domestic travel. When you leave the United States, you need to know your responsibilities under export control regulations as well as be aware of the risks associated with issued travel advisories.

Some foreign governments have regulations that permit the seizure of travelers' computers and the review of their contents. U.S. Customs officials are also authorized to review the contents of travelers' laptops without probable cause and can be held until your return.

It is therefore important to consider the security of UTA equipment and the data and access needs for your purpose of travel in light of these security concerns and export control regulations.

These guidelines help to inform you of the potential risks of traveling abroad, to be prepared when certain situations arise and to use your best judgment when traveling internationally.

Before You Travel Internationally

Review UTA's International Travel Policies & Procedures

- All travel requires prior approval through the Travel Authorization process.
- Travel to countries with an issued travel advisory requires approval from the International Oversight Committee and follows UTA's Policy on Travel to Restricted Regions.
- International Travel **https://secure.compliancebridge.com/utaprod/utaportal/index.php?fuseaction=app.download&policyID=108&doc=BF-T-PR2.pdf&descriptor=header1**

Life and Safety are a Priority: The life and safety of our employees is an absolute priority when travelling to countries outside US jurisdiction and especially to those nations that have received a travel advisory. As an employee traveling on university business, you may be a target for intellectual property theft or other clandestine state-sponsored activity.

A. If you have been approved by the IOC for travel to a location with a travel advisory, exercise caution and always keep family and your department aware of your detailed travel plans and contact information.
B. Always have in hand the number and a means of contacting the U.S. Embassy (or the embassy of your country of citizenship) and verify that the information is correct.
C. Learn about and follow local laws. As a rule, cooperate with border and local law enforcement. If you are detained for any reason, understand and be ready to articulate your rights under the Geneva Convention.
D. Cooperating with law enforcement may mean granting access to your laptop or other electronic devices. You can mitigate improper data access or unauthorized data copying by using a loaner laptop that has been specially prepared for international travel. See laptop loaner program below.

E. In the event that you are compelled by local law to provide your NetID password, offer to log into whatever device they require access. If that is not sufficient and you risk being detained or otherwise feel unsafe, provide your password to them and then contact OIT's help desk at your earliest convenience to have it reset. With two-factor authentication enabled, email via O365 web, UT Share, Canvas and VPN will be protected against unauthorized access.

F. Cybersecurity is of critical importance when traveling internationally. For information on data security while traveling, review the Department of Homeland Security's "Cybersecurity While Traveling Tip Card" and the Center for Internet Security's "Cybersecurity While Traveling".

Considerations for Data Storage, Access, and Transport:

Before traveling, consider the potential for data loss through the loss or theft or, or damage to, the devices taken on travel. Consider how such a data loss will be restored and do not take more data/devices than necessary for the purpose of the visit. The following are all ways in which to help safeguard data and intellectual property. Travelers will need to consider the risks associated with countries and entities being visited.

- Do Not Store Sensitive Data on Internal/External Media: Thieves target travelers and, because of legal issues surrounding the use of encryption as well as customs and border checkpoints, you might not be able to utilize encryption to protect data stored on physical media as you would be able to inside the U.S.

- Use Sanctioned Cloud-Based Storage Over Local Storage: In most cases you will not require your entire library of documents for the duration of your trip. Instead of placing files on local storage, consider using:
  A. Sanctioned cloud-based storage like Microsoft Onedrive to store files. Sanctioned UTA email via web browser instead of using the Microsoft Outlook client. Delete files that are downloaded to the local Downloads folder. UTA email via a web browser requires 2 factor authentication. See instructions for NetId Plus to enroll in 2 factor authentication through DUO.
  B. UTA Sanctioned locations for storing data (Section VI):
- Be Aware of Foreign Import Laws On Encryption: Some countries do not allow cryptography/encryption tools to be imported or used within their borders without a license, or in some extreme cases, at all. Please check with the US Department of State before traveling internationally to ensure that you have the most up-to-date information. Before traveling with an encrypted laptop, check the following websites for more information on international encryption controls:
  The Wassenaar Arrangement
  Bureau of Industry and Security, U.S. Department of Commerce – Export Administration Regulations.

  We strongly recommend the use of loaner laptops when traveling to countries where the import of encryption tools are restricted.

- Use an Encrypted Thumb Drive for Off-Line Storage: For countries that do not have encryption import restrictions (see Import Law section below) and for situations where you anticipate not having internet connectivity (e.g. long-haul flights, rural areas, etc.) consider using a hardware encrypted USB drive for University data, especially if your computer is not encrypted. The ISO recommends the Apricorn brand hardware encrypted drives that can be found on Amazon.com. Thumb drives are easier to manage for the personal use exemption for export control requirements (remains in your possession and control) and is an optimum solution to limit potential data risk/loss (Data/information limited to the specific purpose of the visit).

- Use Loaner Laptops & Handheld Devices: The most significant and effective step you can take to protect your data is to use a loaner laptop specifically designated for travel. It vastly reduces the likelihood that theft or compromise will expose data not relevant to the current trip. It also means that upon your return, the device can be easily erased, helping mitigate the risks of advanced persistent threats. Please contact your department to see if they have any loaner devices available for this purpose.

Be Aware of U.S. Export Control Restrictions: Any travel with or transmission of export controlled (ITAR or EAR) technology or technical data must be cleared through Regulatory Services and described/documented in a Technology Control Plan (TCP). Contact Regulatory Services for more information

Countries of Concern for Foreign Influence: For travel to Countries of Concern for Foreign Influence (China, Russia, North Korea, Iraq), ORS can perform routine checks, screening, and clearances of foreign entities and individuals as part of your travel. It is highly recommended to contact ORS for this screening process when presenting sensitive or unpublished scientific research to these countries (which may or may not require a license under export control laws).

While Traveling Abroad

Use of Wifi or Wired Internet Connections: In general, consider all non-UTA internet connections as not secure; anybody can set up a wireless network and call it whatever they want (and call it “secure”), hoping to lure unsuspecting travelers into connecting. This is especially an issue at airports and hotels, where travelers expect wireless connectivity. The following are best practices when using WiFi abroad:

- Ask an employee at the business or conference if they provide WiFi; if so, what the network name is.
- Don’t connect to rogue networks (unofficial networks set up by individuals in an organization) - this can make it easy for someone to intercept and even alter your communications.
- Turn off wireless when your device is not in use or when network connectivity isn’t required. This keeps your device from broadcasting its presence looking for available networks, as well as associating with an unauthorized network that may share the name of one you have connected to in the past.
- Do not automatically join any wireless networks from laptops or cell phones. Manually pick the specific network you want to join.
- Turn off Bluetooth when it’s not actively being used.

Use UTA’s VPN When Connecting to the Internet: Immediately after connecting to the internet, the first thing you should do is connect to UTA’s VPN. This will create an encrypted connection between your computer and UTA’s network, eliminating the possibility for electronic eavesdropping. For more information on UTA’s VPN: **https://www.uta.edu/vpn**

- You can use VPN to remotely access your UTA computer at work if you need access to data.
- Use VPN even when accessing cloud services like O365, Canvas, UT Share or My Mav.

Avoid Using Non-UTA Issued Computers for UTA Business: Given the prevalence of malicious software and hardware key loggers, and low security standards for most public computers, avoid using them. Always use a UTA issued computer to access UTA data and especially avoid public computers (e.g. internet café, hotel computers, etc.).

Similarly, avoid using personal devices (your own or that of a friend or relative) for storing UTA data. If you must use a personal device, it is mandatory that antivirus software, VPN software and encryption are enabled: **https://www.uta.edu/security/policies/remote_access.php**

Be Aware of U.S. Export Control Restrictions for Presenting or Sharing Information:

If taking or presenting research information while traveling internationally that is not publicly available or fundamental research that is intended to be published, it may have restrictions under export control laws and require a license or confirmation of a license exception. If you are presenting or discussing research, only provide information that is either already published or has no restrictions on publication. The Office of Regulatory Services (ORS) email can be contacted for assistance in these determinations.

Upon Your Return

1. **Very simply, assume that your device(s) have been compromised while traveling abroad and act accordingly.** It can be very difficult to determine if a device has been compromised. Don’t trust the applications on your device and do not use the device to do work or connect to services on campus.
2. If you didn’t travel with a loaner device or a new hard drive, format and reinstall the operating system and applications.
3. **Change all passwords to any accounts that you used to access any services.** Refer to the list you made while traveling to make sure you change them all. Remember to pick strong, complex passwords and do not reuse the same password for multiple services.
4. **Restore your devices to their pre-travel state.** Namely, turn off any services that you enabled specifically to facilitate your work while traveling (e.g. remote desktop).
5. **Report any suspicious activity.** If you were asked to share or provide access to your data, noticed any suspicious activity involving others and your devices, or had inappropriate inquiries to sensitive research/intellectual property, please inform the Assistant Vice President for Research – j.forsberg@uta.edu

a. If you think your devices may have been compromised, consider reinstalling the operating system and reformatting the hard drive.