 Information Technology Security & Compliance

**IT Security for International Travel**

**Guidelines and Checklist**

Given the current climate of dependency on technology, it is important to be aware of current regulations, laws and safety tips to consider when traveling abroad. Additionally, the U.S. federal government has strict policies around export controls which can include technology and some data. More information about this can be found at [FAQ’s for Export Controls](http://www.slu.edu/general-counsel-home/compliance/export-controls/export-controls-faqs) and the [Export Controls webpage.](http://www.slu.edu/general-counsel-home/compliance/export-controls)

To explore various countries travel restrictions, visit <http://travel.state.gov/travel/travel_1744.html>

To maintain contact with work, family, and friends, most persons, when traveling abroad prefer to use mobile electronic communication devices.  Mobile electronic devices such as laptops, cell phones, and tablets, when taken abroad, may be successfully attacked with malware and automated attack tools. These devices, even when kept current with security software, may not be able to thwart such an attack.

Below is a checklist drafted in order to help you prepare for your trip abroad, including tasks to complete when you return to ensure you’ve done the best job of protecting yourself and your data against malicious activity. Even though these guidelines apply to business travel using SLU devices, adopting these best practices for your personal travel is recommended.

|  |  |  |
| --- | --- | --- |
|  | IT Security Travel Abroad Checklist | |
|  | 1. Contact the Export Controls Officer if you plan to travel internationally. There is a TMP form that must be completed. Depending on what [country](#ComprehensiveSanctions) to plan to visit, there may be enforced rules and restrictions in effect. |
|  | 1. Contact CSG or your Distributed IT Admin to borrow a clean loaner laptop. If you are taking your own mobile device, ensure that it has been cleaned before you leave the United States, and immediately after you return. *It is recommended that if you use your own device, you back up your hard drive before your leave.* |
|  | 1. Before you leave, make sure you copy your work files to your respective shared drive so that you can securely access them via University [VPN](https://www.slu.edu/its/software-downloads). In [D1](#D1) countries, you cannot use VPN, but will use Authentic8. The service desk can assist with the installation of this application. |
|  | 1. Secure your laptop or other mobile device with a strong password, OS security updates, [anti-virus](https://www.slu.edu/its/software-downloads), anti-spyware, full disk encryption and firewall software. |
|  | 1. Register your travel plans with your respective supervisor in your department, and ensure your immediate relatives are also aware of your travel plans. Steer clear of discussing too many details of your upcoming trip with the public via social media. |
|  | 1. Ensure you maintain a secure physical environment wherever you are staying. Ensure you securely delete any newly downloaded data from your device prior to leaving your electronics unattended. |
|  | 1. Do not connect to any unsecured Wi-Fi hotspots in the country you are visiting; you should only be accessing University data via VPN or Authentic8. |
|  | 1. Once you return home, ensure devices are completely wiped immediately. Change any of the passwords that you may have used on your trip. Contact the Service Desk for assistance. |

**Countries with clean loaner laptop rules:**

Comprehensive sanctions apply to five countries: Cuba, Iran, N. Korea, Sudan and Syria.  This not only means clean laptop, but any travel to these countries requires a license or exemption from the federal government.

The other countries where a clean laptop would be recommended for export controls would be the D-1 (national security level countries):  Albania, Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam.

Tips about Public Wi-FI:

(<http://www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks>)

Mobile Device Security Tips:

http://www.slu.edu/its/information-security/newsletter-and-tips/mobile-device-security-tips