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 and the Export Controls webpage.

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.

<table>
<thead>
<tr>
<th>IT Security Travel Abroad Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the list of countries that have clean laptop rules to determine if this is a requirement for your trip.</td>
</tr>
<tr>
<td>2. Contact CSG or your Distributed IT Admin to borrow a laptop that has been completely wiped. 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 do use your own device, to back up your hard drive before you prepare for your trip.</td>
</tr>
<tr>
<td>3. Before you leave, make sure you copy your work files to your respective shared drive so that you can securely access them via VPN while traveling.</td>
</tr>
<tr>
<td>4. Secure your laptop or other mobile device with a strong password, OS Security Updates, anti-virus, anti-spyware and firewall software.</td>
</tr>
</tbody>
</table>
5. If legally permitted in the country you’re visiting, ensure the hard drive is encrypted with Saint Louis University standard **PGP encryption.** Do the same for other mobile devices, if supported. If you unsure of your destination’s current laws regarding cryptography, please visit [http://www.cryptolaw.org/](http://www.cryptolaw.org/) for information specific to that country.

   *If the country you’re going to has strict restrictions on this, ensure that you check with your supervisor/professor/trip advisor on what steps you need to take to obtain any permits necessary.*

6. 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.

7. 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.

8. Do not connect to any unsecured Wi-Fi hotspots in the country you are visiting; you should only be accessing University/Sensitive Data via VPN.

9. Once you return home, ensure devices are completely wiped immediately. Change any of the passwords that you may have used on your trip.

**Countries with clean laptop rules or recommendations:**

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:**