Traveling Abroad with your CU Device

When traveling abroad with your CU owned laptop, tablet, or cell phone, there are a few things you need to consider to guarantee the device, along with the data stored on it, is safe and secure.

Before You Travel

Get a Loaner Device

Contact your IT administrator or the Office of Information Technology before traveling out of the country to see if there is a possibility of using a loaner laptop or tablet. The loaner device will ensure that you aren't traveling with a device that has unnecessary sensitive data or your web browsing history. This will give you a clean slate to work from while traveling.

Encrypt Your Device and Protect Data

Prior to traveling, be sure that your device is encrypted and remove or reduce data that you store on your device to only that which is needed to perform job duties. Reducing the amount of data could also reduce the amount of risk associated with traveling with the device.

Encrypt files and data for additional protection. This will help to prevent viewing and use of the data in the event your device is accessed in an unauthorized manner, or by someone other than yourself. It also protects the data from being used in violation of university policies and federal laws such as HIPAA and FERPA that restrict this data to specific use and require authorization. Note: Data reduction or removal should be done in accordance with university records retention policies and applicable federal, state, local laws, and contractual obligations.

Make a secure backup copy of your data before your travel and leave the copy in a safe university provided storage location. This will ensure that the copy is available if data are corrupted or become inaccessible while you travel.

Install and Use the University VPN

Other countries have different web governance rules and restrictions. To ensure a safe and secure internet connection and that you will be able to access university resources, make sure the device you are travelling with has the VPN (called Global Protect) installed. Global Protect will secure your internet connection wherever you are.

Use Duo Two Factor Authentication and Mobile Service Provider

In order to connect to Global Protect (VPN), you will need to ensure that your mobile service provider offers international service. You will need the service to connect to the VPN because the VPN uses two-factor authentication (meaning you will need to either receive a Duo push or Duo call). Two-factor authentication is a safeguard to confirm your identity and verify you are the person signing into the university service.

Learn About Export Control Laws

Some types of technology cannot be taken abroad, so it is important for you to understand United States Export Control Laws. Visit the Office of Regulatory Compliance website for more information, here.

Make Sure Your Software is Up to Date

Check each application on your device to ensure that the latest patches and updates are applied and installed prior to travel. Patch and update software that is not running the latest version or is not current. Out-dated software can be hacked, which could allow an attacker to gain access to your device and its data.

Use Microsoft Defender Software to Detect Malicious Code and Threats

Whether the university device is a loaner or your personal work device, make sure Microsoft Defender is installed on the computer before traveling. Run a full scan of your device before you leave to ensure that there is no malicious code or software that is designed to damage your computer, prevent it from operating appropriately, or allow unauthorized access to your device and data (malware) installed on the device. Microsoft Defender identifies software vulnerabilities, provides antivirus and anti-phishing protection, and detects threats in a single, unified platform. The platform integrates with Microsoft 365 services such as Outlook, SharePoint, and OneDrive, offering robust security. One of the major capabilities of Microsoft Defender is the detection and response functionality which continuously protects computers from malicious activity. This program will help defend against threats while abroad.

Prepare for International Security

Be prepared for your device to be searched or inspected when traveling to other countries. It is also not uncommon to be questioned about your device. Privacy laws in other countries are different as they do not adhere to protections such as those identified in HIPAA and FERPA. Be aware of export controls laws, and do not access sensitive data even while using the VPN if you feel that your connections are not secure.

While You Travel

Avoid Public Wifi

Do not connect to a public wifi network or public hotspots with your university owned device while traveling, such as those found on airplanes, in airports, hotels, train and bus stations, and cafes. And, do not use public wifi to conduct other activities such as personal shopping, banking, or other sensitive activities.

Public wifi and networks are unsecure and unreliable. Connecting to a public network increases the risk of your device being attacked by a hacker, and could lead to identity theft. It is an easy way to cause a breach of data security and for sensitive information to be obtained by an unauthorized user. Instead of connecting to public wifi, use the service provided by your cellular carrier.

Protect Data

Do not download files or data to your university device while you travel. Also, do not accept or use thumb drives or media from other sources as they may be infected with malware.

Disable Bluetooth

Disable Bluetooth on your device to ensure that it does not automatically connect to nearby devices or computers. Re-enable Bluetooth only when you are certain that you are connecting to a safe device.

Use Physical Safeguards

To prevent your university owned device from being stolen, implement the physical safeguards:

- When traveling, make sure that your device is safely secured in your bag. If you don't need to carry your device around with you make sure that your device is locked up either in the safe provided in your room or in luggage with a lock on it.
- Never leave your device unattended.
- Use a privacy screen to ensure that no one can shoulder surf or view the information on your monitor.
- Never charge your device using publicly available charging cables or publicly available USB ports. Cables provided in public locations may be targeted by attackers to transfer the information that you send to their unauthorized networks or systems.
- Do not use publicly accessible computers.

When You Return

Clean or Scan Your Device

When you return from travel, use Microsoft Defender to run a scan against your computer to check for malware or other malicious code infection. If any issues are identified, follow recommendations for remediating them.

Change Your Password

Change your password to a value that is unknown to others when you return from travel. This will ensure that your device and files can only be accessed by you.

Report Security Incidents

If your device is lost, stolen, or you suspect that it has been compromised, notify Information Security immediately.

Instructions for Submitting an Incident:

- Sign in with your CU username and password.
- Click the “Make a Request” button.
- Move the inner right slider all the way to the bottom of the page until you see “Security Event” and click on it.
- Select “Compromised Account” or “Lost/Stolen Device”

For more information, please use these additional resources below:

Cybersecurity While Traveling Tip Card

Cybersecurity Tips for International Travelers

Cybersecurity for Electronic Devices