International Travel - Information Security Guidance

Using laptops and mobile devices helps keep us connected and productive while we are on the road. However, traveling with these devices increases the risks for keeping our personal and Institutional Information private. This webpage provides security guidance on how to keep your information safe while traveling internationally.

*Note: The most important guidance on this page is to travel only with the data and devices that you need.*

Important To Know about International Travel:

There are special rules for bringing electronic equipment, research, intellectual property, and encryption technology abroad. Please consult with Export Controls at exportcontrol@uci.edu well in advance of your trip if you are planning to take University equipment, data, or technology outside the United States.

- Export Controls - International Travel
- Export Controls - Economic and Trade Sanctions (OFAC)
- Export Controls - International Shipping and Hand-Carrying
- UC Traveling Abroad - Training Course
- UCI - Faculty & Staff Travel Resources
- UCI Travel and Disbursements

Before You Leave:

- Bookmark this webpage within your browser or download the PDF version to a device. This way if you ever need any of this information while traveling you will have it available. Check back frequently to make sure you have the latest copy.
  - International Travel - Information Security Guidance
• **Travel only with the data and devices that you need** – especially for international travel. If you don't have it, it can't be stolen or confiscated. This may mean leaving some of your devices at home, removing personal or University data from your devices, or shifting your data to a campus-approved and Multi-Factor Authentication (MFA) protected secure cloud service. If possible avoid traveling with any protected information on your laptop, USB drives, mobile devices, etc.

  ○ For more information around protected information, please visit UCI’s Protection Levels webpage or reach out to securityreviews@uci.edu.

  ○ OneDrive is UCI’s approved cloud storage solution for storing protected information. It is important to enable MFA with OneDrive for an additional layer of security.

    ■ OIT - Getting Started with OneDrive
    ■ OIT - DUO Multi-Factor Authentication

• **Use loaner devices whenever possible.** Consult with your technical support staff to see if there’s an option to borrow a loaner device for your trip.

• **Encrypt all devices and data that you take with you.** Contact your technical support staff for available encryption solutions for your unit. For more information on encryption, please visit OIT Security’s Encryption web page.

  ○ PLEASE NOTE: Encryption is a general recommendation to protect sensitive information in case your device is lost, stolen, inspected, or confiscated, however, it is not okay to bring encryption technology into some countries. Please consult with Export Controls at
exportcontrol@uci.edu if you are planning on using encryption while traveling outside of the United States.

- **Password protect all of your devices.** Use strong passwords, passcodes, or smart-phone touch/facial ID to lock and protect your devices. Set devices to automatically lock after a short period of inactivity.

- **Setup multi-factor authentication** for your accounts whenever possible for an additional layer of security.
  - UCI - DUO Multi-factor Authentication
    - If you don’t have a network connection while traveling, you can still use the DUO Mobile App. Just open the mobile app and use the 6-digit passcode that appears on your screen.
  - UCI - Other Multi-Factor Authentication Options
  - UCI - Multi-Factor Authentication (MFA) FAQs

- **Log out of browsers and apps, remove any saved login credentials and clear your browser history.** This will help prevent anyone from accessing your accounts or information without your knowledge. Also delete apps you no longer use.

- **Update your OS and Apps/software, including antivirus protection,** to make sure you are running the most secure versions available. Contact your IT support staff for guidance if necessary.
  - For additional information please visit OIT Security’s [How to Update Your Computer](https://example.com) webpage.

- **Backup your data.** Whether you are traveling with a loaner computer, your regular computer, tablet or smartphone, you should always backup your data. Store the backup securely in the USA.
○ Reach out to your IT support staff. They may have a backup solution in place and can provide additional guidance.

○ OIT provides fee-based data backup and recovery services for most platforms. Please see OIT Data Backup and Recovery Service for more information.

○ OneDrive, as UCI’s approved cloud storage solution for storing protected information, may also be used to backup data. It is important to enable MFA with OneDrive for an additional layer of security.

  ■ OIT - Getting Started with OneDrive
  ■ OIT - DUO Multi-Factor Authentication

• **Turn on “Find My Device” tracking and/or remote wiping** options in case of loss or theft. Make sure you know how to use these tools before you go. Keep in mind privacy implications of location tracking.

  ○ Find, Lock, or Erase a Lost Android Device
  ○ Erase a device in Find My iPhone on iCloud.com

OIT offers Front Door Software for free to help get lost or stolen devices back. *Please note this product is designed to help retrieve lost or stolen devices, not to provide data security.*

• **Install and configure campus VPN software.** The VPN (virtual private network) allows you to securely connect to UCInet from off campus. Some units may have their own department VPNs, please reach out to your IT support staff for more guidance. For more information around UCI’s Campus VPN, please visit the OIT Campus VPN webpage.
● Set devices to “ask” before joining new wireless networks so you don’t unknowingly connect to insecure or malicious networks.

● Use a webcam cover or tape over the camera of your laptop and mobile device for privacy.

● Review the UC Minimum Security Standard

● Stay informed of TSA regulations. Check State Department’s website for any travel alerts concerning the specific countries you plan to visit (including any tech restrictions) and guidance on travel to high-risk areas. They also provide information for U.S. students traveling abroad, as does the FBI.

While You Are Gone:

● Power off your devices before you arrive at the border. This will help resist a variety of high-tech attacks.

● Do not put devices into checked baggage. Checked baggage can be lost, stolen, or tampered with.

● Always keep your devices with you. Carry devices on the plane, train or bus, and keep them nearby, within your sight. Devices can easily become lost, stolen, or tampered with, especially if you step away or fall asleep. If you absolutely have to leave your device, make sure to turn it off instead of just hibernating it or putting it to sleep.

If you become separated from your equipment, there is a possibility that it has been compromised. If your equipment is confiscated or inspected by any foreign authority, then it should be considered compromised.
If your device is confiscated, lost, or stolen contact your local IT team immediately and visit OIT Security’s Report an Incident web page and follow the directions. You can also contact OIT Security at security@uci.edu.

- **Be careful when using public wireless networks or Wi-Fi hotspots.** Public wireless networks are not secure, anyone could potentially see what you’re doing on your computer or mobile device while you’re connected. If you need Internet access, make sure you know who the reputable carriers are and only connect to them. It is always good to ask the staff at the location for the correct network name before connecting.

If available, utilize **eduroam**. eduroam (education roaming) is the secure worldwide federated network access service developed for the international research and education community. If you are visiting a participating campus, as a UCI affiliate you may use your UCInetID and password to gain access to that institution's wireless network.

- **Use a VPN** (virtual private network) when you’re traveling to make sure your network connection is secure (encrypted). Please see Install and configure campus VPN software.

- **Physically protect yourself, your devices, and any identification documents.** Keep your devices with you at all times during your travels. Do not assume they will be safe in your hotel room or in a hotel safe. Always be aware of your surroundings. Don’t carry bags that are obviously designed to hold laptops or portable devices.

- **Do not plug in untrusted accessories.** Accessories that come from questionable or unknown sources can be infected with malware intended to steal your information. Avoid plugging in any untrusted accessories (flash drive, charging cable/station/port, SD card, power stick, etc.) to your
device. Try to bring all the necessary accessories with you, but if you must purchase something abroad, make sure it is from a reputable source.

- **Never log into anything when using public computers.** Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for its users. Public computers may be loaded with keyloggers and malware.

  If the need to use public computers arises during your travel, avoid entering your credentials. If you use a device belonging to other travelers, colleagues, or friends, do not log in to email or sensitive accounts.

- **Keep track of credentials you used while on travel.** Regardless of whether you are using them on your device or public computer, they may be compromised. To be safe, take note of the credentials you used so you can change them on a trusted and secure device once you return.

- **Disable Wi-Fi, Bluetooth, and GPS when not in use.** This protects you from harmful connections and some types of tracking technology.

- **Wait to post about your trip on social media until you return home.** Using social media while on travel can be risky. You are letting the world know that no one may be at home. Wait to get home before posting pictures or comments about your trip.

**After Your Trip:**

- **Run full antivirus scans on your devices.** Contact your IT support staff for guidance if necessary.

- **Check user account login activity.** UCI has a self-service application that allows you to view your recent UCInetID account activity for common OIT
Services. Verify all the activity is legitimately you. Report any suspicious activity to OIT Security at security@uci.edu

- **Change any and all passwords you may have used abroad.** Regardless of whether you used them on your device or a public computer, they may be compromised.
  
  - To change any of your OIT-managed passwords, please visit [OIT Password Self-Service](#) webpage. You can always contact the [OIT Help Desk](#) if you need assistance (949) 824-2222.

- **Check your statements.** If you used a credit or debit card while traveling, check your monthly statements for any discrepancies for at least one year after you return.

- **Delete unneeded apps.** If you downloaded any apps specifically for your trip and no longer need them, be sure to delete them and the associated data.

Contact Us:

If you need additional guidance please reach out to:

- OIT Security at security@uci.edu.
- Export Controls at exportcontrol@uci.edu

Resources:

- [Export Controls - International Travel](#)
- [Export Controls - Economic and Trade Sanctions (OFAC)](#)
- [Export Controls - International Shipping and Hand-Carrying](#)
- [UC Traveling Abroad - Training Course](#)
- [UC Traveling with Electronic Devices](#)
- [UC Ethics, Compliance, and Audit Services - International Compliance](#)