Travelling with Mobile Devices

The Data Protection Policy helps ensure the protection of the university’s restricted data from unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes.

In order to comply with UC’s Data Protection Policy and federal export control regulations, please follow the checklist below to ensure your device is in compliance.

**Laptops**

- It is recommended that each department has a spare laptop for overseas travel to prevent data scrubbing operational work machines. If one is not available, please contact the UCIT Office of Information Security (OIS) at infosec@uc.edu to request a clean laptop for travel.
- If a clean laptop is not available, or if you prefer to use your own device, digitally scrub (wipe) the hard drive, and reinstall the preferred operating system with the latest security updates, antivirus and firewall. Contact your IT department for assistance.
  - Recommended tool for secure hard drive wiping is [http://www.dban.org/](http://www.dban.org/)
- If data/documents need to be taken overseas, the data owner must first classify the data in accordance to UC’s Data Protection Policy.
- Only take public data during the trip. *Controlled* and *Restricted* data are not authorized to leave the university. If such data is required, please contact the OIS at infosec@uc.edu for further information.
- Some research data is classified as export controlled. If you have any questions about the classification of your data in regards to export controls, contact the OIS at infosec@uc.edu or Institutional Research.
- Use encryption to protect your laptop and external storage from any tampering. **Note:** Depending on your destination, use of encryption may be restricted or disallowed. Please contact the OIS at infosec@uc.edu, especially if you are travelling to Russia, China, former eastern bloc countries, Israel, or any communist country, to check regulations.
- Always use UC’s VPN service to access the internet. Log in at [https://sslvpn.uc.edu](https://sslvpn.uc.edu).
  - This service is used to protect the university's research data, employee information, student records, etc., and make them available only to authorized individuals.
- Do not plug any peripheral devices which you do not own into your laptop.
- At all times, maintain physical possession of your laptop and all peripheral devices.
- If you are taking an external USB device with you, be sure it is free of UC restricted or controlled data and encrypted.
- You may also consult with the OIS for any additional questions.
Cell phones/ Smartphones
- Contained in your cell phone/smartphone is a lot of personal information. This includes phone numbers, text messages, pictures, videos, personal email and work email.
- Do not use a personal cell phone/smartphone while on your overseas travels.
- Consult with the OIS for the various options of cell phone usage during overseas travel.

Tablets
- Tablets can contain personal information as well as data classified under UC’s Data Protection Policy.
- Unless the tablet has been digitally sanitized and restored to factory defaults, or is an entirely brand new tablet that has never been used before, it is not recommended to take a tablet with you during overseas travel.
- If a tablet needs to be taken during overseas travel, it must support the use of encryption and have the ability to use the Junos Pulse (http://www.juniper.net) VPN client to access UC’s VPN services.
  - Android VPN client
    - https://play.google.com/store/apps
  - Apple iOS VPN client
- Do not ROOT or Jailbreak your tablet.
- Do not plug any peripheral devices which you do not own into your tablet if it supports USB.
- At all times, maintain physical possession of your tablet.

Restricted Countries
If you are travelling to North Korea, Iran, Sudan, Cuba, or Syria, contact OIS as soon as possible.