Published on *University of Colorado* (https://www.cu.edu)

Travel Securely with CU Data and Devices [1]

Before Your Travel

Understand international travel requirements

- Your campus may require you to work with the campus Export Control Office when traveling with university property, research data, or specialized software.
- Some countries may restrict encryption technology, research data, or specific applications.
- Contact your campus Export Controls Office if you are unsure what requirements apply.
    - CU Anschutz [2]
    - CU Boulder [3]
    - CU Denver [4]
    - UCCS [5]

Use only what you need

- Travel with the minimum amount of data necessary.
- Remove or avoid storing sensitive or confidential CU data that you will not need during your trip.
    - Review the Data Governance [6]website for more information on data classification.

Verify security protections

- Verify with your IT service desk that your device has whole disk encryption enabled.
- Ensure your operating system, browser and applications are fully updated.
- Confirm antivirus/endpoint protection software is installed and current.
- Enable multi-factor authentication (MFA) on all accounts whenever possible.

Back up important files

- Create a backup copy of work and personal files before traveling.
- Store backups securely using approved cloud storage or an encrypted external drive.
- A backup ensures you can recover your information if your device is lost, stolen or damaged.

While Traveling

Keep devices with you

- Never leave laptops, phones, tablets or removable media unattended.
- Avoid checking devices in luggage whenever possible.
- Keep devices secure in hotel rooms and conference spaces.

Cooperate with border agents' requests to inspect devices

In some countries, border agents may request access to your devices.

- Do not continue using the device for university work afterward.
- Report the incident immediately to your information security office.
- Follow guidance from your campus IT service desk or information security office before reconnecting the device to university systems.

Be careful with public Wi?Fi

- Connect to the CU VPN whenever conducting university business.
- Disable automatic connection to open wireless networks.

Avoid public computers and charging stations

- Do not log into university accounts from public or shared computers.
- Avoid using public USB charging stations [7], which may expose devices to malicious software ("juice jacking").
- Use your own charger and power adapter whenever possible.

Report lost or stolen devices immediately

If a university-owned or personal device used for university work is lost, stolen or compromised:

- Report it immediately [8] to your campus IT service desk or information security office.
- Change passwords for affected accounts as soon as possible.
- Use remote tracking or wipe features, if available.

Need Help?

If you have questions about traveling securely with CU data or devices, contact your campus IT service desk or information security office.

6/1/2026

Groups audience:
Office of Information Security
Right Sidebar:
Information Security Campus Contact
IT Departments Campus Contact
Sub Title:

Whether you’re traveling domestically or internationally for work, protecting university data and the devices you use is essential. Travel increases the risk of device theft, unauthorized access, malware infections, and exposure of sensitive information.

Source URL:https://www.cu.edu/security/travel-securely-cu-data-and-devices

Links
[1] https://www.cu.edu/security/travel-securely-cu-data-and-devices
[2] https://research.cuanschutz.edu/regulatory-compliance/export-control
[3] https://www.colorado.edu/researchinnovation/node/8496/office-export-controls
[4] https://www.ucdenver.edu/services/international-student-and-scholar-services/hr-partners/j-1-scholar/export-control [5] https://osp.uccs.edu/export-controls [6] https://www.cu.edu/data-governance/resources-support/data-classification [7] https://www.cu.edu/security/stay-cybersecure-while-traveling-avoid-public-usb-charging-risks [8] https://www.cu.edu/security/reporting-incident