Office of the Chief Information Security Officer
Risk Advisory: Travel

BACKGROUND

National and international travel are a vital part of the "*boundless*" experience for many members of the UW community. When preparing for a trip, keep the following tips in mind to secure personal and University data and devices.

BEFORE YOU GO

- If possible, acquire temporary devices that are free of personal and University data for use during international travel.
- Record serial numbers on all devices and keep the serial numbers on your person.
- Know what data you have stored on your device. Clear browser caches and temporary files on laptops and other devices.
- Only take the University data you need for your trip. Don't take export-controlled information without proper authorization.
- Use anti-virus software and keep it updated to protect against the latest threats.
- Keep operating systems and applications up to date by applying all critical software patches.
- Back up the University data you'll take with you and leave the copy in a safe place.
- Create a connection to a virtual private network (VPN), such as Husky OnNet. if you need access to University data while you're away. If you're abroad, don't access export-controlled information — even using a VPN.

MOBILE DEVICES

- Keep software, including antivirus, up to date on all devices.
- Protect your devices from physical theft. Never leave your laptop or mobile device unattended. Lock up devices left in hotel rooms.

- On smartphones and tablets, configure automatic tamper and remote wiping, automatic locking, and encryption and use a pass code or PIN to secure the device.
- For laptops and notebooks, protect with a password, use secure transmission mechanisms — such as a VPN — and encrypt your device whenever possible.
- Be aware of the increased risk of malware infection on portable storage devices, e.g., thumb or external hard drives. Scan such devices for malware upon insertion.
- Remove University information from devices when it's no longer needed.
- Turn off your computing devices when not in use and disable WiFi and Bluetooth when not needed. Avoid using hibernation or sleep mode.
- Tape over cameras on devices or disable them while you are not actively using them.

WORKING REMOTELY

- Protect passwords used to remotely access University information, and don't share them with other people.
- Don't use the "remember my password" feature when accessing University information.
- Don't access personal bank accounts, work accounts, or University data from public computers, such as those in libraries, coffee shops, or hotels.

- Be cautious of public wireless networks. Wireless connections that are restricted with a password, or are provided by a trusted source are preferable to public networks. Keep in mind that other people may be able to intercept online activity.
- If possible, avoid downloading software while traveling. In some countries, you may be prompted to download fraudulent "antivirus" or other software. If you are on an extended trip or if updates are needed, go to the software vendor's website to download updates.
- Always delete locally saved files on public or shared computers.
- Use eduroam when connecting to WiFi at participating campuses and institutions around the world.

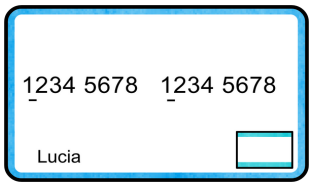
Office of the Chief Information Security Officer
Risk Advisory: Travel

ENCRYPTION

- Use encryption whenever possible when storing or accessing University information on devices.

ADDITIONAL TIPS

- Keep your passport and other personal documents secure from theft.
- Make a copy or take a photo of your passport and keep it in a safe place with you and another copy with a trusted person who is not traveling with you.
- Consider using a credit card with a modest credit limit (rather than your debit card or usual credit card) for use in ATMs that might be susceptible to "skimming" devices.4 Additionally, you may want to contact your bank to inform them about specific travel dates and locations.



- Register with the UW travel registry.
- Learn more about the UW Global Traveler program and how it supports you, including employee travel assistance, student abroad insurance, and international emergency assistance information.

- Learn more about where you are traveling (health, safety and visa requirements) by visiting the U.S Department of State Travel website.

WHEN YOU RETURN

- As a precaution, change any passwords you used while traveling.

PRIVACY AND INTERNATIONAL TRAVELS

Privacy law and regulations vary between countries. Be aware of the applicability of local and international privacy regulations if you are handling personal or confidential information. Depending on where you travel, electronic devices may be subject to review and duplication of data, and encryption of data may be forbidden. Additionally, use of secure websites (those that use "https") or encrypted networks (VPNs) may not be possible.

Office of the Chief Information Security Officer
Risk Advisory: Travel

CONTACT

This list is not exhaustive. For additional information, consult the Office of the CISO or the Office of Global Affairs, UW Global Travelers.

Contact **ciso@uw.edu** or **security@uw.edu** if a device containing University information is lost, stolen, or compromised.

RESOURCES

Description and Information on Export Administration Regulations

Emotet Malware Online Training

Federal Bureau of Investigation: Safety & Security for US Students Traveling Abroad

KrebsonSecurity, All About Skimmers

Mobile Devices Online Training

Working Remotely Risk Advisory