University of South Australia

International Travellers Cyber Security Guideline

Last Updated 23/10/2024.

Contents

This guideline gives clear instructions for staff travelling overseas, including to high-risk countries. It applies to all employees, contractors, and consultants of UniSA who travel internationally and may use company devices or access company networks and data during their trip.

UniSA staff travelling for work, research, or even vacation must take extra care to protect both institutional and personal data on their devices.

Some international destinations are considered hot spots for malicious cyber activity as advised by the Australian Security Intelligence Organisation (ASIO) and the Australian Cyber Security Centre (ACSC). You should be extra vigilant when travelling to these destinations and enact additional precautions prior to and during travel.

For up-to-date destination risk levels, refer to: www.smartraveller.gov.au

Guideline for travel to High-Risk Destinations or for High-Risk Individuals

All travel to **high-risk destinations**, or for a **high-risk individual**[1], you should adhere to the following guideline:

Before you travel

- Complete all UniSA mandatory annual cyber security training and any other training recommended by the cyber security team.

[1] Individuals who, due to their position, research focus, or access to sensitive data, are more likely to be targeted by cyber threats during international travel. This includes faculty, researchers, staff, or students handling confidential information, engaging in high-profile projects, or holding high profile roles.

- Its strongly advised that you do not travel with your current devices used for day-to-day work at the University.
- If you decide to travel with your personal or work device, make sure its software is up to date. It's recommended not to store personal or official data on the device.
- If you require a temporary device, Log a service request with IT Help Desk at least two weeks before your travel to obtain a temporary clean laptop, phone and/or other devices that contains the bare minimum of data, contacts and software required for your trip.
    - You will be required to set up an appointment one week before travelling to receive your temporary devices and ISTS staff will assist you to configure them for use.
    - You will also need to set up an appointment for your planned return date to ensure devices are collected and wiped/destroyed as soon as possible.
    - Mobile devices will support both a physical and electronic SIM card. ISTS staff can assist in configuring as required. Ensure you add any emergency contacts required for your travel to this phone.
    - Enable global roaming on your mobile service – be aware there will be additional charges for this service. Encrypted modems can also be requested if preferred.
- Don't share details of official travel plans or make announcements on social media.
- Ensure Multi-Factor Authentication (MFA) is set up prior to travel and that the authentication method is accessible in the location of travel.
- Secure your devices with a PIN, passphrase or biometrics.
- Enable full tunnel VPN access on your devices. Be aware some countries block VPNs - talk to ISTS staff if you need alternative mechanisms to securely connect.
- Know and follow UniSA policies for using various devices, institutional data, and institutional resources including the UniSA Information Security Policy.
- If you hold a defence security clearance you will need to organise a defence security travel briefing prior to departing by contacting info.defencesecurity@unisa.edu.au.
- If you are provided with a temporary phone SIM please communicate the new contact details to the UniSA Insurance Office (insurance@unisa.edu.au).

While travelling

- Assume any devices that have been taken out of sight for inspection by foreign officials, lost or stolen and later found or returned, to be potentially compromised.
- Users must report any loss, suspected compromised or unusual behaviour (including the type, date, and time) on devices to IT Help Desk desk as soon as possible.
- Never use hotel/in-room safes. Instead, always keep your devices on you.
- Avoid transporting devices in checked baggage and never leave unattended.
- Don't use public Wi-Fi networks. In some countries they're controlled by security services; in all cases they're insecure.
- Never lend devices to untrusted people, even if only briefly (an example would be if an untrusted person asked to check the weather on your device).
- Do not allow untrusted people to charge other devices using their devices (an example would be if an untrusted person asked to charge their phone using your laptop).
- Never use someone else's chargers, cables and other removable devices.

- Turn off Wi-Fi, Bluetooth, and Near Field Communication (NFC) when not in use.
- In locations where sensitive conversations take place, consider turning off devices.
- Avoid re-using removable media after connecting it to other organisation's electronic devices, they could be compromised.
- You must never use any other devices that have been gifted or loaned, especially removable media.

Upon return

- At no time should you connect temporary devices you've been handed to the University network upon return from travel.
- You must change all the passwords you have use while abroad.
- You must return laptop and other devices to IT for re-imaging and return to factory default setting.

Guideline for travel to all destinations

Before you travel

- Review Smartraveller to be abreast of current advisory for your destination.
- Consult with ISTS via IT Help Desk about special concerns regarding your technology or your destinations.
- See if low-cost, loan devices are available to mitigate the risk of losing more valuable equipment.
- Ensure your devices have full disk encryption.
- Enable full tunnel VPN access. Be aware some countries block VPN. Talk to the IT Help Desk for alternatives if needed.
- Set up institutionally approved, centrally provisioned data storage. Note that this storage will only be available if you are connected with the UniSA VPN.
- Disable and place non-transparent tape over the inbuilt webcam.
- Secure your devices with a PIN, passphrase or biometrics.
- Be aware of national data protection laws in your home and destination countries.
- Know and follow UniSA policies for using various devices, institutional data, and institutional resources including the UniSA Information Security Policy.
- Consider purchasing a privacy screen, and country specific plug adapters.

While travelling

- Keep safe by carrying only necessities, keeping bags zipped, and practicing situational awareness.
- Protect mobile devices by keeping them secure, locked, and hidden when not in use.
- Protect RFID-enabled devices and bank cards with RFID shielded containers.
- Report stolen devices to your native embassy or consulate and the UniSA IT Help Desk immediately.

- Protect your data by using privacy screen filters and avoiding public discussions of sensitive data.
- Be wary of public charging stations; use wall outlets with your own chargers or external batteries instead.
- Avoid using courtesy computers in business centres for work-related purposes.
- Disable broadcast services like Wi-Fi access points, Bluetooth devices, and GPS when not needed.
- Don’t connect to unknown resources like Wi-Fi access points and Bluetooth devices.
- Assume locally provided technology, such as wireless networks, may be vulnerable to attacks or have risky security settings.
- Use the UniSA VPN whenever possible.
- Don’t enter sensitive information while connected to wireless hotspots or unsecured networks.
- Use two-factor authentication whenever possible.
- Don’t install software updates or patches while connected to untrusted or unsecured networks.

Upon return

- If you notice unusual activities on your devices, contact the IT Help Desk.
- Provide feedback to the IT Help Desk on what did and did not work well.
- Consider changing your PINs and password.