Flinders UNIVERSITY

Information Technology Services

Overseas Travel Security Directive

The purpose of this document is to establish the minimum set of security requirements for University staff travelling overseas for an approved purpose. This directive will ensure staff adhere to the University's Information Security requirements that will facilitate the ongoing protection of University data and IT systems.

Staff Travel Risks

Mobile devices including laptops, phones, tablets and storage devices are often put at most risk when in transit, particularly when devices are left unattended in hotel rooms, airports and other public places. Intellectual property, confidential personal data and business data are often targeted by thieves in these scenarios. In addition, there is a threat of bringing unwanted malicious software (malware) back to Australia on mobile devices that could adversely impact the University's network. It is vital that staff take measures to prepare for travel throughout the world and take steps to reduces the risks of having data accessed in an unauthorised manner or inadvertently exposing University systems to compromise.

Flinders University staff must ensure the following:

- Sensitive information relating to about research or intellectual property is protected at all times during travel;
- The staff and University are protected from liability regarding regulations that cover some types of research data (for example, the Commonwealth Privacy Act);
- Any requirements relating to non-disclosure agreements and access restrictions are considered;
- Use and transport of electronic and hardcopy information complies with University policies.

Staff should always respect the laws of countries when travelling and be aware that internet restrictions may be in place to prevent access to certain international websites. In the first instance staff are encouraged to avoid travelling with electronic devices or data unless absolutely necessary.

Preparation for Travel

To prepare for travel staff must:

- Minimise the amount of data that is stored on devices to the bare minimum (e.g. reduce email, research materials and documents containing sensitive personal information);
- Leave behind any devices or media (including USB storage) that are not necessary and in the event storage is required ensure it is encrypted with a strong password (at least 8 characters);
- Do not take personal devices that contain University information as these devices may not be configured for maximum security;
- Use separate media for transferring files that will be used overseas and destroy after travel;
- Inventory any data that will be stored during travel and store this in an email or provide to Information Security and Risk (in case a device is stolen or lost);
- Securely back up and store data on media or the University file server;
- Disable wireless technologies such as Bluetooth, Wi-Fi, and GPS when not in use to limit potential unauthorised access to your mobile device;
- Turn off data roaming to prevent excessive charges, in the event mobile data is required overseas, contact the ITS Services Desk to organise a Data Pack that will minimise the costs associated with international mobile data.

Staff may from time to time travel to countries that may expose devices to a higher risk of compromise. China and Russia are considered high risk areas for University travellers as such staff should consider additional precautions (where practical). Theft of devices from hotel rooms and public places including airports and eavesdropping of communications between devices are often perpetrated in these countries to gain access to data. Additional precautions include:

- Maintaining physical control over devices to reduce the risk of data loss. This is especially important where physical security cannot be guaranteed (for example, in airports);
- Taking a loan device during travel as additional means of protecting data. It is recommended that loan devices are erased immediately upon return to Australia (ITS - Client Support can provide loan devices upon request).

During Travel

During any overseas travel staff must take the following steps to ensure the security of devices and information:

- Do not enter or access sensitive data when using a shared or public computer including using VPN or accessing other Flinders websites (which require you to enter your FAN password) and ensure all web browsing utilises secure protocols (e.g. HTTPS);
- Ensure you configure a pin code on mobile devices such as tablets and phones to prevent unauthorised access if a device is lost of stolen;
- Utilise the Flinders VPN service when accessing internal University resources remotely;
- Ensure devices are always in sight or in secured carry-on baggage and screen locks are in use;
- Be particularly careful when inside airports as bags often are searched and never let an official take a device out of sight and never disclose a device passcode or password;
- Avoid connecting USB devices such as iPhones, iPods and portable storage devices, or playing illegitimate CDs or DVDs, unless you are confident that the device is reputable. Gift USB devices, CDs or DVDs are an easy method to distribute malicious software;
- Avoid using public chargers or device docks at hotels or airports.

Staff travelling to Russia or China should also consider utilising a third party Virtual Private Network (VPN) service to secure general network communications and internet access that is designed for use in such countries, such as ExpressVPN or VyprVPN (can be purchased on a subscription basis at $10 per month).

Returning to Australia

When returning from overseas travel staff must:

- Change personal Flinders Authentication Name (FAN) password upon return as a precaution;
- Perform an anti-virus scan of devices to ensure nothing is present before re-connecting equipment to the University network.

Reporting a Security Incident

If a device is lost, stolen or the security of data is suspected to have been compromised the incident must be reported as soon as possible to Information Security and Risk.

It is recommended that staff:

- Contact local authorities to report the loss or theft; and
- Contact Information Security and Risk (ictsecurity@flinders.edu.au) for assistance in changing passwords, locking devices remotely and cancelling phone plans (where applicable).