PSR | Protective Security Requirements

TRAVELLING OVERSEAS WITH ELECTRONIC DEVICES

Introduction

The sophistication and versatility of modern mobile electronic devices means they are often used to extend office functionality outside the workspace and domestic spheres. In terms of convenience, connectivity and increased productivity, the benefits of mobile devices are undeniable. Their use does not however come without increasing risk and they should be used in strict compliance with agency policy and security requirements.

As such, while mobile and electronic device security can be inconvenient, it is essential agencies and personnel actively consider and mitigate the risks of operating mobile and electronic devices overseas.

All electronic devices, whether personal or work, are vulnerable to interception, manipulation and/or information extraction. These risks are heightened overseas. Even personal devices which have not been used to process official information hold a significant amount of information about you. While the compromise of a personal device may not result in the compromise of official information it could still be used maliciously by a hostile agency or individual.

- Agencies should consider whether it is absolutely necessary for a staff member to take their work electronic devices overseas.
- Agency personnel should consider whether it is absolutely necessary to take their personal electronic devices overseas.

If it decided that it is necessary then the guidelines below should be followed where possible.

Personnel should consider taking a “clean” electronic mobile device overseas, that is, a newly purchased device to be used for the length of the trip only and which has not stored any information associated with the user.

Personal Devices

Before traveling you should

- Update the device with the necessary security and application patches.
- Enable device security features such as access passwords and PINs.

During travel you should

- Never use your personal mobile or electronic device(s) for official business.
- Maintain physical control of electronic devices at all times; if a device is taken out of your sight or physical control, treat it as compromised. This includes storage in hotel safes and checked-in luggage.
- Practice security awareness; do not allow strangers to access or handle any electronic devices in your possession and be alert to any covert access to information stored on them, for example, onlookers attempting to read the screen.

Work Devices

In addition to the guidelines outlined for personal devices above, if taking and operating a work electronic device overseas, personnel should comply with the following measures.

Before travel you should

- Remove any official information stored on the device that is not required.

During travel you should

- Not use work devices to access or process sensitive or official material in public locations, for example, in hotel lobbies, airports or while using public transportation.
- If the device is not being used, especially during classified conversations, consider disabling wireless and Bluetooth functions and powering the device off and/or removing the battery.
- If your electronic device is taken out of your sight or physical control, treat the device as compromised and cease to use it.
- Use the device for work and/or official purposes only, not for personal purposes.

After travel you should

- Report any compromise of an electronic device – either suspected or actual – to the agency Chief Security Officer as soon as possible and have the device sanitised before it is used again.