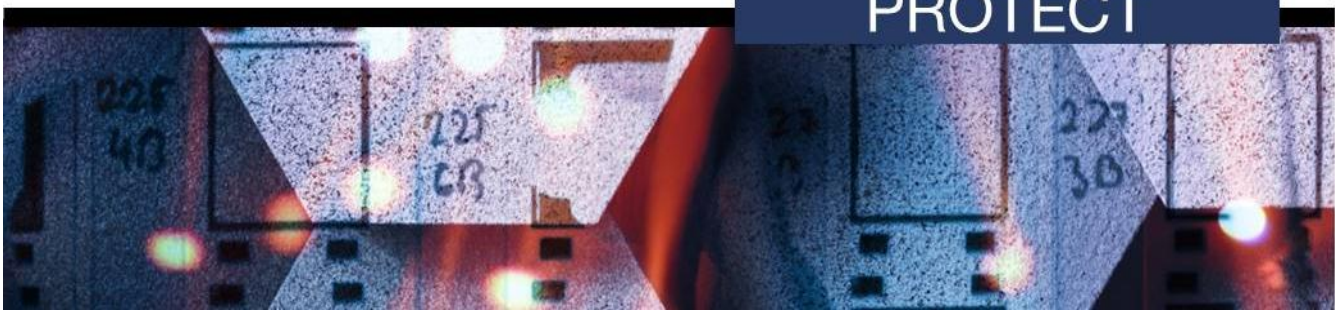

DECEMBER 2012

Travelling Overseas with Electronic Devices (User Guidance)

Introduction

1. All employees should ensure they carefully consider security risks when using electronic devices while overseas. The compromise of devices could have an impact on your organisation, its information and its reputation. In most countries you have no expectation of privacy in internet cafes, hotels, offices or public places.
2. Your IT staff should assist you prior to travelling, however when you are travelling it is your responsibility to ensure the security of your information. This document provides steps to take before, during and after you travel to maximise the security of devices and the information held on them.
3. This advice complements the physical security guidance in the *Protective Security Policy Framework* (PSPF) as well as the *Australian Government Information Security Manual* (ISM).
4. The information is this publication also complements the guidance in the *Travelling Overseas with Electronic Devices (Technical Guidance)* publication available from the Australian Cyber Security Centre (ACSC) website.

Before you travel

5. Consult IT staff prior to departure. They can confirm that each device's configuration is correct and that all updates, patches, encryption and antivirus software have been installed. They may also advise on further security measures such as emergency information sanitisation procedures if you are travelling to a high-risk location.
6. If IT staff provide you with an organisation-owned device(s), ask them to explain to you what has been done to maximise its security and any restrictions on its use. IT security staff will be able to conduct a risk assessment for devices being taken overseas. This information will help you understand the environment and level of risk to devices and the information they hold.
7. Remove all non-essential data from devices. In particular, reconsider the need to take sensitive or classified information overseas.
8. Disable any feature or software that is not required for the trip. The less software on devices, the smaller the opportunity to exploit and gain access to devices through software vulnerabilities.

9. Disable Bluetooth and wireless capabilities and the ability to ‘auto-join’ a network. This will prevent devices from inadvertently connecting to untrusted networks.
10. Ensure strong passwords are used. A password should be either a long simple password (at least 12 alphabetic characters) or a complex password (at least 9 characters featuring a combination of upper and lower case characters, numbers and symbols). This guidance is based on requirements outlined in the ISM. However, organisations should consult any available device-specific hardening guides, as password policies may differ from the advice in the ISM. A password should never be written down and stored with a device. For devices such as smart phones, tablets and laptops enable a short automatic screen-lock after which the password will automatically need to be re-entered.
11. Back-up your data before you travel. If a device becomes compromised, you may not have the opportunity to recover data from it.

While you are travelling

12. Maintain physical control over devices, not only to minimise the risk of theft or loss, but also to protect the confidentiality of information stored on devices. It is advisable to keep devices in your possession at all times and not trust hotels or other services to provide physical protection of devices. Never check your devices in as luggage; devices should be taken onto the plane as hand luggage.
13. Do not connect to open Wi-Fi networks for business purposes. Only wireless communications that are needed and can be secured should be enabled. Instead, connect back to your organisation via a Virtual Private Network (VPN) to use the Internet. This ensures that all browsing traffic goes through your organisation’s internet gateway and is subject to normal security controls implemented by your organisation.
14. Do not use devices to store or communicate information above its approved sensitivity or classification level. This includes sending information via email.
15. Where possible, avoid using a non-organisation controlled web-based email service, such as Gmail, Hotmail or Yahoo, for business purposes. Using such services for business purposes can increase the risk of unauthorised disclosure of business information, as well as bypass any security measures your organisation has put in place to protect your devices.
16. Clear your web browser after each use. This includes deleting the history files, cache, cookies, URL and temporary internet files. This should ensure that there is no remaining information available should someone else obtain access to a device.
17. Avoid connecting USB devices such as iPhones, iPods and portable storage devices, or playing illegitimate CDs and DVDs unless you are confident that the device is reputable. Gifted USB devices, CDs or DVDs are an easy method to distribute malicious software.

When you return

18. Upon return, advise your IT security staff if the device was taken out of your possession for any reason, particularly if you have travelled to a high-risk location. Also advise them if you left any device in your hotel room for an extended period of time. IT security staff should be able to check devices for any malicious software or evidence of compromise. As best practice, all passwords associated with devices should be changed upon return from overseas travel.

Further information

19. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

20. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

21. Additional platform-specific hardening guides are available on the Australian Cyber Security Centre website to assist organisations in the secure configuration of devices. This guidance is available at https://www.acsc.gov.au/publications/.

Contact details

22. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).