Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE

PROTECT

FEBRUARY 2017

# Travelling overseas with an electronic device

1. All Government employees should ensure they carefully consider information security risks when using an electronic device while overseas. The compromise of your device could have an impact on your department, its information and its reputation. In most countries you have no expectation of privacy in Internet cafes, hotels, offices or public places.

2. This advice complements the physical security advice in the *Australian Government Protective Security Policy Framework* as well as the *Australian Government Information Security Manual* (ISM).

3. Your IT department will 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 your electronic device and the information held on it.

## Before you travel

4. Consult your IT security staff prior to departure. They can confirm that your 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.

5. If your IT staff are providing you with an agency device such as a laptop, ask them to explain to you what has been done to maximise the information security of the device and any restrictions on its use. IT security staff will be able to conduct a risk assessment for the equipment being taken overseas. This information will help you understand the environment and level of risk to your device and the information it holds.

6. Remove all non-essential data from the device. In particular, reconsider the need to take sensitive (for example Sensitive: Cabinet) or classified information overseas.

7. Disable any feature or software that is not required for the trip. The less software on the device, the smaller the opportunity to exploit and gain access to the device through software vulnerabilities.

8. Disable Bluetooth and wireless capabilities and the ability to 'auto-join' a network. This will prevent your device from inadvertently connecting to untrusted networks.

9. 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, agencies should consult available device-specific guidance, such as that contained in ASD hardening guides, as password policies may differ from the generic advice in the ISM. A password should never be written down and stored with the device. For devices such as smart phones and tablet PCs enable a short automatic screen-lock after which the password will automatically need to be re-entered.

10. Back-up your data before you travel. If your device becomes compromised, you may not have the opportunity to recover data from it.

## While you are travelling

11. 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 the device. It is advisable to keep your device in your possession at all times and not trust hotels or other services to provide physical protection of equipment. Never check your device in as luggage; devices should be taken onto the plane as hand luggage.

12. 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 agency Virtual Private Network (VPN) to use the Internet. This ensures that all browsing traffic goes through your agency’s Internet gateway and is subject to normal security controls implemented by your agency.

13. Do not use the device to store or communicate information above the classification of the device. This includes sending information via email.

14. Where possible, avoid using a non-agency controlled web-based email service, such as Gmail, Hotmail or Yahoo, for business purposes. Using such services for conducting government business can increase the risk of unauthorised disclosure of official information, as well as bypass any security measures your agency has put in place to protect your device. Malicious cyber actors are also known to send socially engineered emails from webmail accounts. Using a webmail account for work purposes makes recipients more likely to accept a socially engineered email that has a business related subject.

15. 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 the device.

16. 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

17. 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 country. Also advise them if you left your device in your hotel room for an extended period of time. IT security staff should be able to check the device for any malicious software or evidence of compromise.

18. As best practice, all passwords associated with a mobile device should be changed upon return from overseas travel.

## Further information

19. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.asd.gov.au/infosec/ism/index.htm

20. Hardening guidance for specific devices including Apple iOS and Blackberry can be found on the ASD public website at www.asd.gov.au.

21. This information complements the advice in ASD's Technical advice: *Travelling overseas with an agency issued electronic device* publication, available on the ASD public website.

## Contact details

22. Australian government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

23. Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.