Information Security

Safeguarding information away from the office or abroad

Guideline

Assists with fulfilling information security obligations when working remotely or travelling on business.

Keywords:	Information security, travel, international, remote.	
Identifier: SEC GUIDE 04	**Version no.:** 1.0	**Status:** Final
Issue date: 7 February 2014	**Date of effect:** 7 February 2014	**Next review date:** July 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

Background

Having access to Official Information[1] and other government information assets (such as systems, devices, software and services) when working remotely or travelling on business is a fundamental requirement. Information security is not designed to impede the business, but rather to ensure it is conducted responsibly. Responsible handling of information engenders trust and confidence, which in turn results in positive business outcomes.

This guideline outlines the key information security considerations to factor in to your travel and remote working (teleworking) plans. Personnel, including contractors and suppliers with contractual obligations requiring adherence to the Information Security Management Framework (ISMF), are accountable for maintaining the security and appropriate handling of Official Information at all times.

Guidance

This guideline assists individuals and responsible parties in fulfilling their information security obligations when working remotely or travelling on business. Implementing the guidance in this document will assist in meeting the requirements of the Victorian Government information security policies and standards:

- SEC POL 01 Information Security Management Policy
- SEC STD 01 Information Security Management Framework

Overview

Information is the lifeblood of any organisation. Some information may be more valuable or sensitive and this is indicated within government by its classification. Irrespective of whether you are intending to work around the corner at your preferred coffee shop, in an airport lounge while waiting to catch a domestic flight, about to embark on an overseas trade mission or to attend a conference, or even working from home, there are common requirements and expectations of Victorian government personnel and other responsible parties when Official Information is being used outside of the regular office environment.

Espionage and criminal organisations target personnel to extract information of value or interest using a combination of technology, social networks, listening devices, physical surveillance and opportunistic solicitation or phishing to obtain information about individuals, government spending, finances and plans, to obtain commercial advantage or to advance other interests that may be contrary to the objectives of your agency, Victoria or national interests. This guideline provides a comprehensive but not exhaustive list of precautions and risk measures that can be applied when working with information outside of your regular office environment.

Requirements

All business and social engagements present an opportunity for individuals, be they foreign operatives, political activists, commercial entities or criminals, to acquire information. When travelling or working outside of the office environment, the risk of becoming a victim can be reduced by considering the following actions:

[1] any information developed, received or collected by, or on behalf of, the Government, through its agencies and contracted providers

Before you leave or travel with Official Information

(including that stored on mobile devices such as telephones, tablets and laptops or USB memory sticks etc.)

- Review the publicly accessible information that exists about you as an individual. Your presence on social media, public internet sites and membership lists or publications may describe where you work, and the nature of work you undertake, increasing the likelihood that you are a 'person of interest' and may be exposed to targeted surveillance to obtain any sensitive information or knowledge that you possess.

- Avoid using the social media features of travel organiser software (such as TripIt, Worldmate, Kayak, Traxo and the like) to broadcast your precise dates, locations and travel intentions on the web.

- Only take the minimum amount of information you require to conduct your affairs in public locations or while abroad.

- Ensure that sensitive information that is not required remains within or is transferred to your office environment or stored securely on removable media within your office and is removed and permanently deleted from your portable devices that you intend to take with you.

- When necessary, verify or confirm with your Agency Information and Technology Security Adviser (ITSA), that the classification of information you require when outside of the office does not exceed the classification of your mobile device. For example, do not store PROTECTED information on a mobile device or USB key that has only been secured and configured to support For Official Use Only information and data.

- Disable or remove 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.

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

While in public places or in transit

(bus, train, airports, planes, hotels etc.)

- Carry all sensitive information irrespective of the form (paper documents, computers, mobile devices, CD Roms etc.) on your person. Never check it in or leave the devices unattended.

- Avoid storing Official Information unattended in rooms or stored in hotel room safes or at safety deposit boxes with reception.

- Ensure that information which is Sensitive or Security Classified has been encrypted.

- Power off electronic devices (as far as practicable) when they are not being used. Any device that is 'on' is subject to interception and intrusion attempts.

- Exercise extreme caution in public locations when discussing business matters, whether on the phone, texting or typing or in person.

- Recognise the possibility that some airport, airline and transport operators may have close ties or loose affiliations with intelligence services.

While visiting external organisations, office premises and hotels/convention centres

- Fax (facsimile) machines are a particularly poor means of exchanging sensitive information. Not only are fax machines readily intercepted over public communications networks, but by virtue of their nature, result in sensitive information being left unattended for prolonged periods and possibly intercepted or copied by unauthorised parties. The recipient's fax can be collected by anyone so there is no assured delivery, and many machines store a digital image of sent and received pages even after the original fax has been received and removed from the device.

- Consider the possibility of covert listening and video recording devices in general areas, meeting rooms and conference areas. Treat your login, password and on-screen information as you would your personal banking PIN.

- Do not plug your information assets into unknown devices (such as docking stations provided in hotel rooms and lobbies).

- Do not permit others to plug their unknown devices into your information assets (e.g. *'Can I just put my USB key in your machine to give you these files?'; 'May I just charge my phone on your computer?')*

Additional requirements and considerations for international travel

When travelling internationally, you will be subject to the prevailing laws of the jurisdictions in which you are travelling, and you may be subject to interception, covert surveillance or additional measures not just from 'host nation operatives' and criminal organisations but from other individuals involved in global espionage, surveillance or intelligence gathering.

- While espionage does occur on Australian territory, personnel travelling abroad may also be vulnerable. A foreign government can operate more easily and with greater impunity within its own borders, making hotel rooms, restaurants, offices, and telecommunications systems vulnerable to espionage activities.

- Be aware that intelligence services can garner information about you from multiple sources prior to your departure from Australia. Sources may include the internet, a visa application, a list of conference or trade event attendees, hotels and limousine operators. You may be under surveillance from the moment you enter another country.

- Only take information with you that is essential to your affairs while abroad.

- Your risk assessment process for overseas travel should factor in information security, including classification and sensitivity of data/information that will be required for the journey. Arrange a security briefing with your Agency Security Executive and determine the need for a briefing by the Cyber Security Officer for the Victorian Government, Office of the Chief Technology Advocate within Department of State Development, Business and Innovation. The briefing will address the

proportionate risks and measures to be taken according to the information you are travelling with, your ultimate destination, and the transit points for your planned journey.

- Advise your agency ITSA and/or Agency Security Security Executive immediately if an information asset has been lost, stolen, or you suspect that it has been compromised in some way or any time your information asset has been taken for 'inspection' or removed from your presence by foreign customs officials.

- Advise your agency ITSA and/or Agency Security Security Executive immediately if any of your devices were taken out of your possession for any reason. IT security staff should be able to check the device for any malicious software or evidence of compromise.

- As best practice precaution, all passwords associated with mobile devices should be changed upon return from overseas travel.

When 'free' is costly: gifts, services and other enticements

Many facilities, products and complimentary services offered to travelers may expose you to digital espionage. Consider carefully use of the following services proportionate to the information you carry or access from remote locations:

- Public Internet and 'Wi-Fi hotspots' may intercept and log your keystrokes on a computer or your network traffic as it is passed from their network to the internet. While affordable Internet access may be an enticement, use of these services should be governed by some degree of wariness:
    - If the environment (such as a café or lounge) appears suspect, avoid using the services.
    - When using free services, limit the scope of your communications to information exchange that is not Sensitive or Security Classified in nature.
    - Observe your Internet browser and tablet devices for abnormal behaviour, for example, random cursor movement, quickly appearing then disappearing pop-up windows or boxes, broken padlocks or warning messages appearing in your browser that normally do not appear.

- Public storage services offered by concierge, reception or within hotel rooms may be subject to interception or tampering while you are away from the immediate area.

- Baggage and luggage handling services offered at airports or hotels effectively takes assets out of your direct control. Sensitive or Security Classified Information assets should not be entrusted outside of your direct control.

- Free USB keys, CD-Roms and software may contain malicious code known as 'malware' which is designed to steal, harm or otherwise compromise your electronic security. By all means accept the items, but it is highly advised to refrain from using any of them, until you have returned to your regular office environment and have had the item appropriately scanned and declared free of malware by your ICT professionals.

It won't happen to me (but can you be certain of that?)

Intelligence and criminal entities understand the 'value chain' of information, and that the best way to obtain sensitive information is never in a straight line but rather a circuitous complex web of connections and social interactions with personnel at any level within the target organisation.

Obtaining information is about establishing 'connections'. The nature of information surveillance and gathering is that information grows in value and sensitivity as more is obtained. No matter the level, position, time you've worked at a location, what you do for work or perception of your value as an employee, you can be certain that you are a starting point to obtain further information in the 'value-chain'.

Reference and toolkits

- Travelling overseas with an electronic device (Department of Defence Australian Signals Directorate): http://www.asd.gov.au/publications/csocprotect/electronic_devices_os_travel.htm
- Technical advice for travelling overseas with an agency-issued electronic device (Department of Defence Australian Signals Directorate): http://www.asd.gov.au/publications/csocprotect/electronic_devices_os_travel_tech_advice.htm
- Smart Traveller website – Australian Government: http://www.smarttraveller.gov.au/
- Espionage when travelling abroad – what are the risks? (Government of the Netherlands) & Digital espionage – what are the risks? (Government of the Netherlands): https://www.aivd.nl/english/publications-press/aivd-publications/@1587/three-publications/
- Victorian Government Information Security documents: http://www.digital.vic.gov.au/policies-standards-guidelines/information-security/
- Australian Government Protective Security Policy Framework [PSPF]: http://www.protectivesecurity.gov.au/

Further information

For further information regarding this standard, please contact digital.government@dsdbi.vic.gov.au.

Version history

Version	Date	TRIM ref	Details
1.0	February 2013		Adapted from the Office of the Chief Information Officer, Government of South Australia material on International Travel Safeguarding information (ISMF Guideline 16).