SACSF/G13.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline – Cyber security when travelling overseas

Purpose

Cyber security is fundamental to the successful operations of the Government of South Australia. South Australian (SA) Government agencies are responsible for ensuring that any SA Government employees or suppliers that access SA Government information and resources, including when travelling overseas, are doing so in alignment with the requirements defined in the South Australian Cyber Security Framework (SACSF).

This document is intended to provide guidance on the practices and processes that SA Government agencies should follow when they have personnel travelling overseas. This includes guidance for securing electronic devices before, during and after travel.

This guideline should be read in conjunction with the Cyber Security Overseas Travel Checklist (Appendix 1), which has been developed as advice for personnel to follow when travelling overseas.

For more specific advice, please contact the Cyber Security Directorate, Office of the Chief Information Officer (OCIO) at CyberSecurity@sa.gov.au.

Scope

This guideline applies to:

- all SA Government agencies and personnel operating on behalf of the agencies
- suppliers and non-government personnel that access SA Government information and resources.

The SACSF policy statements related to this guideline are:

- **SACSF Policy Statement 2.13: Teleworking –** Secure practices for teleworking must be established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.

Guideline detail

Travelling internationally can pose significant risks to the SA Government due to the potential for information stored on or accessible through electronic devices, including computers or mobile devices, being targeted by malicious actors to access sensitive information or compromise SA Government systems.

Due to this risk, the SACSF includes requirements relating to teleworking for SA Government personnel travelling overseas, with controls to be implemented in alignment with the risk of travel, including the destination country.

Before departure

The following sections provide guidance that agencies should consider prior to the departure of SA Government personnel travelling overseas.

Risk assessment

A risk assessment should be performed when agencies become aware of the intent for personnel to travel overseas to understand if the travel is considered high risk. This should consider the position currently held by the traveller, the sensitivity of the information required to be taken overseas or being accessed during the travel, and the travel destination. An agency should consider the overseas travel to be **high risk** where it meets any of the following criteria:

- Personnel holding a high risk position such as Minister, Executive or Director.
- Personnel with access to or intending to take information classified OFFICIAL: Sensitive or above (including information stored on devices).
- Personnel travelling to a high risk country in accordance with Smart Traveller advice (where Advice Level is classified as Do not travel, Reconsider your need to travel, or exercise a high degree of caution).

Where the overseas travel is deemed **high risk**, agencies may choose to contact OCIO directly (cybersecurity@sa.gov.au) for assistance with a cyber security risk assessment, advice on any specific requirements to address the risks identified, or assistance with a cyber security travel briefing.

High risk travel

If the overseas travel is deemed **high risk**, the following should be considered prior to departure:

- Provision of specific ‘clean’ travel device/s for use overseas (to replace the traveller’s usual device). This may include phones, tablets, and laptops.
- Provision of dedicated travel accounts with only the minimum amount of access and information required.
- Provide guidance to personnel around the consideration of not taking their own personal electronic devices, especially if the devices are jailbroken.
- Apply Security and Construction and Equipment Committee (SCEC) endorsed tamper seals to key areas on agency-owned electronic devices, such as hard drive bays, removeable media slots or any other external interfaces that could be tampered with.

- Hold a formal security briefing for personnel travelling overseas with consideration of cyber security guidance to ensure they understand the associated risks and measures to be taken in accordance with this risk.
- Increase user account monitoring for indicators of compromise for personnel travelling overseas during the dates of travel. Contact OCIO for assistance with options for additional monitoring.
- Perform any other measures identified via the agency or OCIO risk assessment process.

This guidance is in addition to the following general guidance, and any other specific requirements provided by the Security and Emergency Recovery Management team or OCIO following their risk assessment.

General guidance

Agencies should consider the following general guidance prior to departure for all overseas travel:

- Ensure personnel are aware of the Department of the Premier and Cabinet Cyber Security Overseas Travel Checklist (Appendix A) and associated advice to give clear understanding of good security practices while travelling abroad.
- Record details of any agency-owned electronic devices being taken overseas, such as product type, serial/model numbers and International Mobile Equipment Identity into an asset inventory.
- Ensure all agency-owned devices are running vendor supported Operating Systems that are fully patched and securely configured with non-essential accounts, information and functionality removed.
- Based on the risk assessment, consider the use of additional layers of protection to encrypt traffic and data (for example, use of a VPN to encrypt all mobile device communications).
- Configure remote locate and wipe capabilities of electronic devices and ensure they are encrypted, including when locked if possible, and using pre-boot authentication.

Returning personnel

Agencies should consider the following general guidance on the return of personnel with agency-owned devices:

- Reset user credentials that were used with electronic devices or for remote access.
- Monitor user accounts of personnel that have recently returned from overseas travel for indicators of account compromise. Pay close attention to failed login attempts using the recently reset credentials or successful logins from overseas.
- If appropriate, sanitise all removable media used by travelling personnel and decommission multi-factor authentication tokens that have left the physical possession of personnel.

Where the travel was considered **high risk**:

- Ensure that personnel return any ‘clean’ travel devices provisioned separately by the agency’s ICT Service Desk.

- Sanitise and reimage agency provisioned or owned electronic devices as per agency procedures.
- Perform any other measures identified via the risk assessment process.

Personal overseas travel

Usually, staff travelling overseas for holidays or personal reasons don’t need access to SA Government information. However, in some cases there may be legitimate business reasons to consider granting access.

Even though the travel is not work-related, the same cyber security risks to government and government information are present. If the overseas access is approved by the agency, the risk assessment and mitigations listed in this guideline should be applied.

The use of Conditional Access policies to restrict access to M365 by location (including access to email, SharePoint and Teams), and geo-blocking other applications, can reduce risks associated with unapproved overseas access to government information. This will also ensure that staff undertake an approval process, as they will not be able to access government systems from overseas without prior approval and risk mitigations being in place.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- Premier and Cabinet Circular – PC030 Protective Security in the Government of South Australia (PDF 321 KB)
- South Australian Protective Security Framework
- South Australian Cyber Security Framework
- Smart Traveller
- Travelling overseas with electronic devices (Australian Cyber Security Centre)
- Premier and Cabinet Circular – PC040 Air Travel (PDF 230 KB)

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Government Chief Information Security Officer	
Email: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.0	Original approval: September 2023
Next review date: September 2024	Last approval: September 2023

Licence

Government of South Australia
Department of the Premier and Cabinet

Cyber security overseas travel checklist

Travelling overseas for business or leisure presents greater cyber security risks, especially when travelling with personal or work devices. This checklist provides guidance on how to stay cyber safe while travelling to protect personal and South Australian Government information before, during and after your trip.

Before you leave

- □ Understand the value of your information and only take the minimum required with you.
- □ If you intend to travel with a government-owned device, notify your agency's ICT Service Desk with at least two weeks' notice before travelling overseas (where possible), and provide them with destinations and dates of travel. Your agency will determine if you are travelling to a high-risk destination and may provide specific travel devices, email accounts, and/or advice for your travel.
- □ Review your posts on social media and ensure any sensitive information is set to private. If travelling for business purposes, don't post details of your trip to social media.
- □ For personal devices, ensure your anti-virus software is up to date and software updates have been applied.
- □ Uninstall or disable any features or apps that are not required for your trip (for example, Bluetooth, social media apps).
- □ Consult with your agency's ICT Service Desk about purchasing a data plan to be used overseas to avoid using public Wi-Fi.
- □ Ensure you use strong unique passwords for your personal and work-related devices and accounts. Use multi-factor authentication and an approved password manager.
- □ Note the contact details for your agency security team and ICT Service Desk in case you need to report a lost, stolen or compromised device. Also make sure you know how to contact local emergency services, and contact details for the nearest Australian diplomatic mission if you need assistance. If your destination doesn't have an Australian diplomatic mission, find out in advance which country can help Australian citizens. Keep these contact details with you at all times.

While overseas

- ✓ Always carry all devices and sensitive information with you. Don't leave them unattended, including in your luggage or hotel room. Take care not to leave them in taxis or airplanes.
- ✓ Avoid connecting devices to public Wi-Fi networks, such as in the airport, hotel or internet café, as they are generally unsecured connections. Connect using the method provided by your agency (for example, mobile data plan and VPN).
- ✓ Use your work issued device to access SA Government information and services. Avoid using untrusted devices.

✓ Disable any communication capability for your devices (for example, Bluetooth, NFC and Wi-Fi) when not in use and turn off your devices when going through security checkpoints or in sensitive areas.

✓ Do not plug untrusted cables or accessories (for example, USBs, chargers etc.) into your devices, including at designated charging stations in airports, as these may contain malware.

✓ Do not let untrusted people borrow or use your devices, even to check the weather, sport scores or to make a quick phone call.

✓ Avoid viewing sensitive work information on your device or having work-related conversations in public spaces or unsecure areas such as airports, onboard airplanes, in hotel lobbies and public vehicles.

✓ If you receive any suspicious emails, do not click on links or open attachments. Report them immediately to your agency's ICT Service Desk.

✓ Report any lost or stolen device/s immediately to your agency's ICT Service Desk.

✓ If you encounter any suspicious behaviour while overseas, contact your agency security team who will help you to lodge a report with the appropriate authorities. For example, if your device is taken out of your sight for security screening at the airport or at a security checkpoint, comply with directions from officials, and notify your agency security team.

When you return

□ If you were provided with a loan device by your agency's ICT Service Desk or any other requirements to mitigate risk, ensure you return the device without connecting it to your work network and/or follow other provided instructions.

□ Contact your agency's ICT Service Desk to reset all passwords and pins on devices or accounts you used overseas. You may also wish to reset your passwords for your personal accounts.

□ Complete the Post Overseas Travel Security Report and return it to sapsf@sa.gov.au.

□ Remain alert for unusual behaviour on your devices (for example, overheating, missing files, inaccessible files or popups) or suspicious emails with links or attachments. If you notice anything suspicious, report it immediately via your agency's ICT Service Desk.

For more information

- Visit Smart Traveller (www.smartraveller.gov.au) for advice about the risks you might face overseas, including country specific advice.
- Visit the Australian Cyber Security Centre's website (www.cyber.gov.au) for security advice including travelling overseas with an electronic device.
- If you have any other concerns before, during or after your travels overseas, contact your agency IT Security Adviser.

Cyber Security Directorate	**T** 1300 244 168
Office of the Chief information Officer	**E** CyberSecurity@sa.gov.au
Department of the Premier and Cabinet	**W** dpc.sa.gov.au