SACSF/G14.0
GOVERNMENT GUIDELINE ON CYBER SECURITY

# SACSF Guideline – Employees based offshore

## Purpose

Government of South Australia (SA) agencies are responsible for ensuring that any employees or suppliers that access SA Government information and resources, including while based overseas, are doing so in alignment with the associated risks and requirements defined in the South Australian Cyber Security Framework (SACSF).

The SACSF has been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

The SA Government has a small number of employees living and working outside of Australia. These employees generally work externally to the SA Government Microsoft 365 central tenancy, have different email addresses than the standard ‘sa.gov.au' email address, and receive general technical support from third-party service providers.

This guideline is intended to provide advice to agencies on how to best manage the cyber security risks associated with remote-working employees to protect the confidentiality, integrity and availability of government information assets.

## Scope

This guideline applies to:

- all Government of South Australia agencies and personnel operating on behalf of SA Government agencies.

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

### Considerations

To reduce the attack surface, and prevent government data and systems being compromised while employees are working overseas, agencies should consider the following guidance:

- Ensure all offices, regardless of location, are incorporated into the overall Cyber Security Program for that agency and are not managed separately. This should include, but is not limited to, alignment with requirements as defined by the SACSF and the South Australian Protective Security Framework (SAPSF).
- Perform a risk assessment to ensure that the unique risks of working from a specific office are considered and appropriate controls are implemented in accordance with the risk (refer SACSF Guideline 13.0 Cyber security when travelling overseas (PDF 330 KB)). Include any risk advice received from government agencies such as Department of the Premier and Cabinet, Department of Foreign Affairs and Trade, Department of Home Affairs, or the Australian Cyber Security Centre.

  Review the risk assessment periodically or when significant changes occur in the work environment (change of location, travel alert for that country, etc.).

- Consider the guidance provided in SACSF Guideline 7.0 Remote and home-based teleworking (PDF 280 KB) with respect to accessing SA Government systems and information outside of the office, which includes requirements relating to Bring Your Own Device (BYOD), device management, remote access, access to information, video conferencing, systems and operations, and network communications.
- Provision access for overseas-based workers as per agency standard practices. Ensure staff working remotely are aware of the process to submit requests for account-related issues to their agency's ICT Service Desk (where possible), while still seeking general technical support from local service providers. Consider the need to implement supervised monitoring for any service provider to undertake remote administration work, to limit the risk of being compromised.
- Develop and maintain a register of any employees based overseas, including any electronic devices in their possession and any other work-issued equipment, such as product type, serial/model numbers and International Mobile Equipment Identity into an asset inventory.
- Include specific contractual requirements and considerations related to cyber security in any agreement with a service provider, as well as conduct a risk assessment prior to formal engagement with that provider (refer SACSF Guideline 3.0 Engaging Suppliers and Cloud Security (PDF 358 KB)).
- In addition to the requirements defined in the SACSF and SAPSF, consider implementation of the following with respect to physical security:
    - Physical security measures proportionate to the assessed business impact of harm or compromise to agency resources.
    - Facilities to ensure secure storage and disposal of data, information, and assets.
    - Appropriate visitor management controls, including escorting of visitors in alignment with the classification of information.

**Employee awareness**

To prevent the compromise of SA Government information, provide your overseas employees with clear guidance and awareness on cyber security considerations specific to overseas work. This should include consideration of the following:

- Embed offshore workers into standard agency specific cyber security awareness training.
- Provide additional awareness training for SA Government employees working overseas that provides coverage of:
    - increased risk of them being a potential target for foreign state threat actors
    - who to contact in the event of a cyber security incident or suspicious event (both for offshore workers and any locally based service providers)
    - the physical security risks, especially when working in a shared office space, relating to tailgating into office spaces or secure areas, locking of devices when unattended, ensuring devices are not left in unsecured areas, and clear processes relating to the visitors in office spaces, including appropriate supervision
    - SACSF Guideline 13.0 Cyber security when travelling overseas (PDF 330 KB) and associated advice to give a clear understanding of good security practices while travelling abroad
    - how to manage the risks associated with the use of personal devices for work purposes, including avoiding the storage of SA Government information on personal devices.

## 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
- SACSF Guideline 13.0 Cyber security when travelling overseas (PDF 330 KB)
- SACSF Guideline 7.0 Remote and home-based teleworking (PDF 280 KB)
- SACSF Guideline 3.0 Engaging Suppliers and Cloud Security (PDF 358 KB)

## Definitions

| Term | Definition |
|---|---|
| Bring Your Own Device (BYOD) | An organisational policy that allows employees to use their own personal devices for work purposes. These devices |

| Term | Definition |
| --- | --- |
| | connect to and utilise the organisation's network, data and resources. |

## Acronyms

| Acronym | Words |
| --- | --- |
| SACSF | South Australian Cyber Security Framework |

## DOCUMENT CONTROL

| | |
| --- | --- |
| Approved by: CIO Steering Committee | |
| Contact: Government Chief Information Security Officer | |
| Division: Cyber Security Directorate - OCIO | Compliance: Optional |
| Review number: V1.0 | Original approval: September 2023 |
| Next review date: September 2024 | Last approval: September 2023 |