



SACSF/G7.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 7.0: Remote working

Purpose

Cyber security is fundamental to the successful operations of the South Australian (SA) Government. The [South Australian Cyber Security Framework](#) (SACSF) and supporting guidelines have been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government public sector agencies.

This guideline has been developed to assist agencies and applicable suppliers to understand and implement the privileged access management requirements of the SACSF.

Scope

This guideline applies to:

- SA Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

The SACSF policy statements related to this guideline are:

- **SACSF Policy Statement 2.12: Mobile Device Management** - Technical and procedural controls are in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.
- **SACSF Policy Statement 2.13 Teleworking** - Secure practices for teleworking are established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.
- **SACSF Policy Statement 2.4 Access to Information** - Access to agency systems, applications and information is based on business need, authorised by the information owner or delegated custodian and is limited to the minimum required for personnel to undertake their duties. Secure authentication mechanisms are in place to control access to agency systems, applications and information.



- **SACSF Policy Statement 2.6 Robust ICT Systems and Operations** - Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.
- **SACSF Policy Statement 2.8 Network Communications** - Network communications must be secured, ensuring agency information traversing internal and external networks must be appropriately protected based on its classification and can only be accessed by authorised parties.

Background

The SA Government offers its employees a variety of flexible working arrangements. The suitability of these flexible work options is dependent upon the nature of an employee's work, the needs of the business unit, the employee's circumstances and respective employment conditions.

Some departments allow employees to work from a location other than the primary workplace. Remote working involves employees making use of technology to connect to government systems from outside of the office. This guideline assists agencies in ensuring that information assets used for remote working are adequately meeting government confidentiality, integrity and availability requirements, and the SACSF.

Notwithstanding the benefits to employers and employees, remote working adds a new dimension of risk to the security of government information assets.

In accordance with the SA Protective Security Framework, agencies are responsible for developing and implementing policies and processes to ensure the security of persons, assets and information associated with remote working activities.

Guideline detail

Administrative and technical measures should be implemented for the conduct of remote working and include the following processes and areas:

- governance
- bring-your-own-device (BYOD)
- device management
- remote access
- security awareness
- access to information
- video conferencing
- systems and operations
- network communications

Refer to the table below for guideline details.

Considerations

Governance

- Establish a formally endorsed remote working policy, or include statements in an existing policy that:
 - designate an internal point of contact for approval, oversight, management and implementation
 - establish employee and vendor expectations and responsibilities
 - identify IT equipment permitted in the remote working context
 - incorporate other agency policies and procedures
 - outline disciplinary actions for policy violations.
- Identify employees who require remote access to perform critical security functions and provide dedicated access, where possible. If a dedicated path is not available, remote access sessions for the identified staff should be prioritised to ensure they always have access.
- Include statements in an 'acceptable use' or similar policy that address:
 - if BYOD is an appropriate practice, and if so, include guidelines for staff using personal assets to conduct official business
 - the need to follow all policies and procedures set by the agency, regardless of where work is performed.
- Ensure the revocation of authority, access rights and the return of equipment when remote working activities cease is incorporated into existing agency procedures.
- Include cyber security considerations in business continuity plans.
- Develop and test a cyber security incident response plan that includes how your agency would respond to an incident that affects workstations on a remote network.

Bring-your-own-device (BYOD)

- Subject to the information classification and nature of the work involved, agencies may elect to restrict or limit the use of personal equipment for work-based activities.
- Agencies must be well equipped to monitor and respond to any potential security risks introduced by staff using personal ICT equipment to connect to government networks and systems.
- Where possible, dedicated, and controlled equipment should be provided by the agency.

Device management

- Configure remote locate and wipe capabilities of electronic devices and ensure they are encrypted, including when locked if possible, and using pre-boot authentication.
- For international travel, travel devices are provisioned to staff in alignment with the risks associated with the destination country/countries. If appropriate, agency employees should be issued with newly provisioned accounts and electronic devices from a pool of dedicated devices to be used solely for work-related activities.¹
- Record details of electronic devices such as product type, serial number and International Mobile Equipment Identity (IMEI) in an inventory of electronic devices being taken.
- Ensure electronic devices are running a vendor-supported operating system that is fully patched and securely configured with all non-essential accounts, information and functionality removed.
- Ensure that when a device is no longer required by an employee for remote working, it is returned to the agency for re-deployment.
- Ensure a mechanism is in place to patch vulnerabilities assessed as 'extreme' within 48 hours of release.
- Ensure response plans are prepared to mitigate the increase of cybersecurity activities, including log review, attack detection, and incident response and recovery.
- Configure devices to automatically update endpoint detection and response applications.
- Ensure that staff connect to a trusted WiFi, and do not connect via untrusted or public WiFi.

Remote access

- Update Virtual Private Network (VPN), network infrastructure devices and all applicable devices with the latest software patches and security configurations.
- Consider implementing a jump server for personnel to perform administrative activities. When implementing a jump server to protect critical resources, multi-factor authentication and strict device communication restrictions should be used.
- All remote connections should utilise multi-factor authentication to increase security.
- Test remote access solutions capacity or increase capacity where possible.
- Ensure remote plans are always up-to-date, and access systems are regularly patched.
- Ensure key personnel have dedicated or prioritised access to systems to facilitate the performance of critical security tasks.

¹ See SACSf [G13.0 Cyber security when travelling overseas \(PDF 382 KB\)](#) and [SACSf G14.0 Employees based offshore \(PDF 211 KB\)](#) for more details on employees working remotely from overseas.

Security awareness	• Personnel accessing official information and other information assets away from the office must treat those resources with the same level of care and discretion as if working in their usual environment. • Increase awareness of cyber security for your staff, including what they need to consider, where they can go for help and how can they report any suspicious activities. • Ensure staff are aware of security incident notification and response procedures and be on heightened alert to respond to a suspected security incident.
Access to information	• Ensure staff have the necessary training before remote working so they can confidently and securely access information that is relevant to their work. • All public servants must use multi-factor authentication to connect to government networks when working remotely. • Consider the classification of your agency information, how that information is accessed and where it is stored. There may be some agency information that is not appropriate to be accessed from outside of the office. • Consider whether staff should be able to print information away from the office.
Video conferencing	• Undertake a risk assessment on all video conferencing platforms prior to use. • Ensure only verified attendees are participating in meetings by requiring users to authenticate when joining.
Systems and operations	• Some systems may not be accessible remotely or require a VPN. Check whether your security policies or systems configurations are compatible with remote system administration and advise staff accordingly. • Be prepared with an alternate option in the event network configurations and data restrictions affect remote patching options, domain authentication and group policy updates for remote users. • Ensure agency employees are aware that changing their network password while using their home network means it may not synchronise to the device. • As files that are saved onto local machines will not be backed up, ensure that staff are aware of where they need to store files, and that storage complies with record management requirements. • Changes in remote access arrangements may affect logging and may cause an increase in false positives due to increased remote user access. Ensure you can still authenticate users and log actions in systems. • Ensure that network communications and device event logs are sent to a centralised logging facility for monitoring and detection of malicious cyber activity.

Network communications

- Ensure that network architecture is documented showing the incoming and outgoing egress points used by devices accessing devices remotely.
- Risk assessments are performed for all information flows associated with critical processes and appropriate controls applied.
- Ensure that network communications traversing external networks can be sent by an encrypted transport security layer.

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

- [ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements](#)
- [ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls](#)
- [South Australian Cyber Security Framework \(SACSF\)](#)
- [South Australian Protective Security Framework \(SAPSF\)](#)
- [SACSF G13.0 Cyber security when travelling overseas \(PDF 382 KB\)](#)
- [SACSF G14.0 Employees based offshore \(PDF 211 KB\)](#)
- [Australian Cyber Security Centre - Information Security Manual \(ISM\)](#)
- [Australian Cyber Security Centre – Essential Eight](#)
- [PC030 Protective Security for the Government of South Australia \(PDF 322 KB\)](#)
- [Code of Ethics for the South Australian Public Sector](#)

Definitions

Term	Definition
Remote Work	The use of technology to connect to official government networks from a place other than the office for the purpose of official work
Telework	For the purpose of this guideline, telework is the same as remote work.

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework
BYOD	Bring-your-own-device
IMEI	International Mobile Equipment Identity
VPN	Virtual Private Network

DOCUMENT CONTROL

Approved by: CIO Steering Committee

Contact: Government Chief Information Security Officer

Division: Office of the Chief Information Officer

Compliance: Optional

Review number: V1.1

Date of approval: 24 April 2024

Next review date: April 2025

Original approval: November 2021

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite the Office of the Chief Information Officer, Department of the Premier and Cabinet, Government of South Australia, 2024.

