SACSF/G7.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 7.0: Remote and home-based teleworking

Introduction

Cyber security is fundamental to the successful operations of the South Australian (SA) Government. Cyber security risks are evolving, as rapid technological advances lead to an increased reliance on technology to perform critical business functions. The management and effective sharing of information and information technology resources is essential to maintain legal and regulatory compliance, reputational image, and meet the objectives of the SA Government.

The South Australian Cyber Security Framework (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.

Applicability

The SACSF applies to:

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

Scope

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 the respective employment conditions.

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

Notwithstanding the benefits to employers and employees, teleworking adds a much greater risk to the security of government information assets.

In accordance with *PC030 Protective Security in the Government of South Australia* (PC030) and the *South Australian Cyber Security Framework* (SACSF), agencies are responsible for developing and implementing policies and procedures to ensure the security of persons, assets and information associated with teleworking activities. Staff compliance is the responsibility of agency chief executives, as per *PC030.*

The Commissioner for Public Employment has issued Commissioner's Standards that include general provisions relating to working at home.

The SACSF policy statements related to this guideline include:

- **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.

Considerations

Governance

- Establish a formally endorsed teleworking 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 telework context
    - incorporate other agency policies and procedures
    - outlines 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 ‘bring-your-own-device’ (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 teleworking activities cease is incorporated into existing agency procedures.
- Include cyber security considerations for staff working remotely in business continuity plans.
- Develop and test a cyber security incident response plan that includes how your agency would detect, respond and recover 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 should monitor and respond to any potential security risks introduced by staff using personal ICT equipment to access government information.
- Where possible, dedicated and managed equipment should be provided by the agency.
- Employees who connect to cloud-based government systems using their personal devices should comply with the South Australian Public Sector Code of Ethics related to appropriate handling of official information and use of government resources.

Device management

- Configure remote locate and wipe capabilities of work-issued electronic devices and ensure they are encrypted, including when locked if possible, and using pre-boot authentication.
- Travel devices are provisioned to staff for international travel 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.
- Record details of all work-issued electronic devices such as product type, serial number and International Mobile Equipment Identity (IMEI) in a central asset register.
- 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 a staff member for teleworking, 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 cybersecurity activities, including log review, attack detection, and incident response and recovery.
- Configure devices to automatically update endpoint detection and response applications.

Remote access

- Update Virtual Private Network (VPN), network infrastructure devices and all applicable devices with the latest software patches and security configurations.
- 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 external connections should utilise multi-factor authentication to maintain appropriate security.
- Test remote access solutions capacity or increase capacity where possible.
- Ensure VPN and other 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.

Security awareness

- Personnel accessing official information and other information assets away from the office should 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 data 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 should 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

- Check whether your security policies or systems configurations are compatible with remote system administration and advise staff accordingly.
- Network configurations should not impact the ability for remote patching, domain authentication and group policy updates for employees who are teleworking.

- Ensure agency employees are aware that changes to network passwords while working remotely can result in synchronisation issues.
- Staff should store files in line with agency and state government record management requirements, making use of cloud-based systems such as Microsoft Office 365, noting that files saved locally may not be backed up.
- Any file saved by employees on local drives must be securely removed at the end of their tenure with the SA Government.
- Changes in remote access arrangements and more employees working from home may affect logging and cause an increase in false positives. Ensure you can still authenticate users and log actions in systems.
- Ensure that network communications and device event logs on work-issued devices 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/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.

Departments and agencies should ensure that their cyber security posture is maintained. Should any controls be relaxed, a risk assessment should be undertaken and mitigation controls put into place if required.

This guideline does not aim to provide the reader with a complete list of responsibilities, obligations and controls associated with teleworking. The individual requirements of agencies will have direct bearing on what measures are implemented to mitigate identified risks.

References, links and additional information

- PC030 Protective Security for the Government of South Australia
- South Australian Cyber Security Framework
- Code of Ethics for the South Australian Public Sector

Document Control

ID	*SACSF/G7.0*
Version	*1.0*
Classification/DLM	*OFFICIAL*
Compliance	*Discretionary*
Original authorisation date	*November 2021*
Last approval date	*November 2021*
Next review date	*November 2022*

Licence