SACSF/G2.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

Suppliers using the South Australian Cyber Security Framework

Purpose

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.

This guideline will support suppliers who access, process, store, or otherwise handle digital information on behalf of a South Australian Government agency to understand the expectations of them under the SACSF.

Scope

The SACSF applies to:

- South Australian 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 provide services to agencies.

Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency.

Supplier access is defined as any local or remote access made by a supplier to government information and communication technology (ICT) assets. In terms of arrangements with suppliers, the scope extends to the various service delivery interfaces with those suppliers, as defined in contracts and/or service level agreements. It includes auditing of security services

implemented by suppliers that have a material impact on the security of information managed by the agency, but otherwise excludes the suppliers' internal processes.

The SACSF policy statement directly related to this guideline is:1.5 Supplier Management:

- *Cyber security requirements must be included in all agreements with suppliers. Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework*.

Agency responsibilities

Prior to engaging with a supplier, agencies should perform an assessment of the risks introduced by the supplier and ensure appropriate risk mitigation and technical controls are implemented. For more detailed information on managing cyber security risks introduced by suppliers, refer to SACSF Guideline 3.0 Engaging Suppliers and Cloud Security.

Supplier responsibilities

Suppliers should provide supporting information to enable agencies to complete a risk assessment so that they can meet the supplier management requirements of the SACSF.

Suppliers are expected to:

- Understand agency expectations regarding security requirements of any agency information and systems to which they may have physical or logical access.
- Apply controls documented in contracts or service level agreements (SLA) with the agency, commensurate with the classification of the information and systems that are to be covered by the service to be provided. This can include, but is not limited to:
    - formally documenting policy and procedural controls or enhancing existing documentation to meet the agency's requirements,
    - implementing or enhancing technical security controls, including segregating agency information from information of other clients held by the supplier,
    - providing suitable security awareness education to all supplier personnel who may be providing services to the agency,
    - performing background verification checks as required by the agency relative to the classification of the agency information and systems which may be accessed.
- Provide supporting evidence to the agency that the controls documented in the contract or SLA are implemented and effective. This will be expected:
    - prior to commencing the engagement with an agency, and
    - periodically thereafter as per the contractual agreement with the agency.
- Sign a non-disclosure agreement which will extend indefinitely unless otherwise noted.

- Understand incident reporting requirements detailed in *PC042 – Cyber Security Incident Management* and *SACSF G4.0 Cyber Security event and incident reporting*. Suppliers must have processes in place to report any cyber security incidents impacting South Australian Government information, services or ICT infrastructure to the agency that they are contracting with and the Department of the Premier and Cabinet.

Suppliers should note that:

- Agency information must not be provided to any third party, including sub-contractors, other than the supplier unless express written approval from the agency is obtained. Approval must be sought from both the contract manager and an appropriate executive or security adviser.
- Agencies will reserve the right to terminate access to information and systems at any given time, however suppliers are also required to notify the agency when access is no longer required.
- Where privileged access to systems is required to perform contracted services, suppliers will be required to follow documented agency processes for requesting access each time it is required, and this access should be revoked whenever it is not in use.
- Where suppliers are providing technology security services, periodic competency vetting of supplier personnel should be performed by agencies in line with contractual agreements and SLAs.

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

- South Australian Cyber Security Framework (SACSF)
- SACSF Guideline 3.0 Engaging Suppliers and Cloud Security
- SACSF G4.0 Cyber Security event and incident reporting
- PC030 Protective Security in the Government of South Australia
- PC042 Cyber Security Incident Management

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.1	Original approval: November 2019
Next review date: July 2024	Last approval: July 2023