



SACSF/G3.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 3.0: Engaging Suppliers

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 agencies.

This guideline explains the practices and procedures that SA Government agencies are expected to follow when engaging the services of suppliers, contractors or other third parties to access, process, store, or otherwise handle digital information on their behalf.

Scope

The SACSF 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 who provide services to agencies.

Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a SA 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.

Guideline

For an agency to meet the expectations for *SACSF Policy Statement 1.5 Supplier Management* when engaging suppliers, they must ensure they identify and manage the cyber security risks introduced by those suppliers.

Below are considerations that may apply to a broad range of contractual arrangements. Agencies should consider which of these considerations are applicable to their specific arrangements and risk profile. For information specific to cloud security, see [SACSF Guideline 18.0 Cloud security](#).

Prior to engaging with a supplier, agencies should:

- Perform an assessment of the potential information security risks introduced by the supplier. A supplier security questionnaire to assist with this assessment is available in the Security SA Teams site.
- Define and document the risk mitigation activities and technical security controls required of both the supplier and the agency in a formal supplier agreement. These controls should:
 - be commensurate with the classification of the information assets to be protected,
 - align to the agency's risk appetite and risk management framework,
 - address the system and information access requirements of the supplier (including any additional third parties providing services to the supplier).
- Define and document the supplier's assurance reporting requirements in the contract or service level agreement (SLA), based on the agency's risk assessment.
- Ensure the security requirements in the contract and/or SLA with the supplier are reviewed and approved by the agency or government's legal, procurement or appropriate other representative before execution.
- Ensure an appropriate non-disclosure agreement is in place if required.
- Obtain evidence of relevant background verification checks of supplier personnel with access to agency information or agency IT assets from the supplier if required.

Contractual considerations

Agencies should ensure that the contract terms with suppliers address any data sovereignty issues. Specifically, the terms should establish and agree the location of all agency data held by the supplier, considering:

- the location of the primary data store
- replication of data to support high-availability solutions and/or authentication
- online and offline backup locations
- administration and support staff who may access data
- requirement to advise the agency of any changes that may impact data sovereignty.

The contract or SLA should also consider other key issues to the satisfaction of the agency (as the information owner). Depending on the service being contracted these may include:

- Certification to an auditable information security standard such as ISO 27001 or SOC 2, and a requirement to provide evidence of certification periodically.
- Arrangements for the SA Government to obtain independent assurance of security controls specified in the contract (right to audit).
- Requirements for the supplier to have a level of cyber security insurance to assist them to recover from a cyber security incident that may impact their ability to provide services to SA Government.
- The legal jurisdiction applicable to any dispute.
- Requirements to meet the agency and government information management requirements ([State Records](#)) including identifying ownership, legal possession and custody of information assets.
- Specification of record keeping functionality and metadata requirements to meet regulatory and business record keeping requirements.
- The storage and use of personal information meets the requirements of the Premier and Cabinet Circular [PC012 South Australian Government's Information Privacy Principles Instruction](#) and any applicable legislation.
- Requirements of [South Australian Protective Security Framework](#) in relation to security controls for information based on classification, and [SACSF Ruling 2 Offshore data storage and processing](#).
- Assurance that the supplier cannot use SA Government information for applications not specified in the contract. For example, it cannot be on-sold or otherwise used for marketing purposes.
- Requirements to consult with the agency regarding any third party seeking to have access to agency information.
- Requirements to have a security incident management plan that includes a process to advise the agency of any incident that may impact confidentiality, integrity or availability of agency information within 24 hours, and a requirement to work with SA Government to respond to the incident. This should consider [PC042 – Cyber Security Incident Management](#) and [SACSF G4.0 Cyber Security event and incident reporting](#).
- Service resilience controls, such as:
- Requirements that systems and services be supported by current business continuity plans that are tested periodically.
- Agreeing Maximum Allowable Outage (MAO) and Recovery Point Objectives (RPO) in the SLA.
- Data security controls, such as:
- Maintaining audit logs of all access to SA Government information.
- Encryption of information in transit and at rest – in particular sensitive and personal information.
- Maintaining vulnerability management and patching processes for all systems storing, processing or communicating SA Government information.

- Ensuring physical protections are in place to prevent unauthorised access to SA government information.
- Ensuring all access to sensitive government information is authorised and protected by robust access management controls including multi-factor authentication.
- The contract should also specify the supplier's obligations at the completion of the contract / on exit from the arrangement, including:
 - return of all specified information and associated metadata to the agency in an accessible nominated format(s),
 - assurance that no copy of the agency's information is retained by the supplier, and
 - requirements for the secure sanitisation or disposal of data storage that has hosted agency data (primary storage and backup media).

During engagement with a supplier, agencies should:

- Periodically obtain evidence from suppliers that they have maintained the required security controls as documented in the relevant supplier agreement.
- Periodically obtaining evidence from the supplier of their cyber security program maturity.
- Performing periodic vetting of the supplier's competency specific to the role they are performing for the agency in place of internal agency resources.
- Obtain assurance that the supplier has met their contractual obligations and implemented the controls documented in the contract and/or SLA.

Upon completing an engagement with a supplier, agencies should:

- Reinforce the supplier's ongoing contractual cyber security obligations, including non-disclosure agreements which must extend indefinitely unless otherwise noted.
- Obtain evidence that no SA Government information is retained by the supplier and that all requirements for secure sanitisation or disposal of media and data have been met.

Register of suppliers

Agencies are expected to maintain a register of suppliers providing services that may impact the confidentiality, integrity and availability of agency information and systems. The following is an example of the type of information that should be captured for each supplier:

Description	Example
• Description of services provided by the supplier	• Support for server infrastructure
• Classification of information assets that the supplier has access to	• OFFICIAL: Sensitive • Moderate Integrity • High Availability

OFFICIAL

Does the supplier have access to Personal Information	Yes
Criticality of the service to the agency	High
Agreement information (type of agreement, next review date, reviewer, location of the agreement)	- Master Services Agreement last reviewed by [IT Manager] on [DD/MM/YYYY]. [Document location]
Nature of the logical and physical access that the supplier has to agency information	- Full physical access to server infrastructure. - No logical access – hardware support only
The degree of confidence that the agency has in the security controls and terms in the contract	High
Description of the risks to the business	- Unavailability of data centre may result in major interruption to critical services - Significant reputational damage
Supplier risk assessment conducted	Yes – (date)
Minimum supplier requirements as documented in the agreement	- ISO 27001 certification 99.99% uptime on data centre service - Physical and environmental control status reports

Using and maintaining a register will ensure agencies have visibility over who their suppliers are together with their respective security obligations. A supplier register template is available in the Security SA Teams site.

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](#)
- [South Australian Protective Security Framework](#)
- [Government of South Australia Cloud Services Policies and Guidelines](#)
- [PC012 South Australian Government's Information Privacy Principles Instruction](#)
- [Procurement Services SA](#)

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework
SLA	Service Level Agreement
ICT	Information and Communication Technology

DOCUMENT CONTROL

Approved by: CIO Steering Committee

Contact: Chief Information Security Officer

Division: Office of the Chief Information Officer Compliance: Optional

Review number: V1.2 FINAL Original approval: November 2019

Next review date: October 2026 Last approval: November 2024

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 Treasury and Finance, Government of South Australia, 2024.