SACSF/G3.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

Engaging Suppliers and Cloud Security

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.

These guidelines explain the practices and procedures that South Australian 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:

- 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*.

Guideline

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

Prior to engaging with a supplier, agencies should:

- Perform an assessment of the potential risks introduced by the supplier. A guiding 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.

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.

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
• 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.

Cloud security guidance

Further to the requirements above, this section provides additional guidance with respect to the use of cloud service providers.

Background

- Cloud services provide a range of potential benefits for many agencies including cost, scalability, and flexibility of platform and capacity. Using such services may also allow agencies to better focus on their core business, leaving aspects such as IT infrastructure management to specialised service providers.
- However, outsourcing introduces different risks to the agency given the loss of direct control over aspects of service delivery, as well as reduced visibility over any breakdown in controls that may occur. Sharing the responsibility between the agency and the cloud service provider may also add to the level of risk, particularly where the separation is not well defined and understood by all parties.
- The adopted cloud service model (Infrastructure/Platform/Software as a Service) will impact the responsibilities that are retained in-house and those that are outsourced. In any case, there is potential that neither party will undertake some key activities that fall 'between' the stakeholders, and the impact may only become obvious after a serious

failure has occurred. The cloud deployment model (public, private, community or hybrid cloud) may also impact the control options that are available to manage information security risks associated with the service.

Agency responsibility

- Responsibility for risk management remains primarily with the agency, even where activities are performed by a cloud service provider.
- Checks and balances must be implemented by the agency to maintain an appropriate level of assurance that the service provider has appropriate processes in place to:
    - manage the security of agency information in line with government policy and expectations
    - perform the activities for which the service provider is responsible.

Contractual considerations

Agencies should ensure that the contract terms with cloud service providers address any data sovereignty issues. Specifically, the terms should establish and agree the location of all agency data held by the cloud service provider, 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 the processing environment and data.

The contract should also consider other key issues to the satisfaction of the agency (as the information owner) including:

- Requirements to meet the agency and government information management requirements (State Records) including identifying ownership, legal possession and custody of information assets
- Requirements of South Australian Protective Security Framework in relation to security controls for information based on classification, and SACSF R2.0 Storage and Processing of Information in Outsourced and Offshore ICT Arrangements
- Specification of record keeping functionality and metadata requirements to meet regulatory and business record keeping requirements
- The storage and use of personally identifiable information meets the requirements of the Premier and Cabinet Circular PC012 South Australian Government's Information Privacy Principles Instruction
- Assurance that the cloud service provider cannot use tenant data for applications not specified in the contract. For example, it cannot be on-sold or otherwise used for marketing purposes. It must not be used to data match with databases owned by other clients of the cloud service provider

- Assurance that no copy of the agency's records or information is retained by the cloud service provider after the termination of the contract (including secure destruction of data in line with records management requirements)
- Requirements for the secure sanitisation or disposal of data storage that has hosted agency data (primary storage and backup media)
- Requirement to advise the agency of any incident that may impact confidentiality, integrity or availability of Agency data and allow the Agency to manage communications in compliance with *PC042 – Cyber Security Incident Management* and *SACSF G4.0 Cyber Security event and incident reporting*
- Requirement to advise the agency of any changes that may impact data sovereignty
- Requirements to consult with the agency regarding any third party seeking to have access to tenant records
- The legal jurisdiction applicable to any dispute
- The contract must also specify the cloud service provider'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).

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

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