# SACSF Guideline – Suppliers using the SACSF

## Introduction

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

The SACSF is a risk-based framework, developed to assist with preserving the confidentiality, integrity and availability of information by applying risk management processes, with increasing control measures implemented based on increased likelihood or impact.

## Applicability

The SACSF applies to:

- All South Australian State Government Agencies and personnel operating on behalf on the Agencies.
- Non-government suppliers and personnel that access South Australian State Government information and resources.

The SACSF covers both:

- Information and communications technology (ICT) systems, and
- Industrial automation and control systems (IACS) that handle government or personal data or provide critical services to the state.

## Scope

These guidelines will support suppliers who access, process, store, or otherwise handle information on behalf of a South Australian Government Agency.

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 IT 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.

# Supplier Guidelines

## Background

Prior to engaging with a supplier, Agencies must perform an assessment of the risks introduced by the supplier and ensure appropriate risk mitigation processes and technical controls are implemented.

## Supplier Requirements

Suppliers will be required to provide supporting information to enable Agencies to complete the assessment and ensure they are adequately meeting the supplier management requirements of the SACSF.

Suppliers will be required 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 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 SLA are implemented and effective. This will be required:
    - 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 SACSF Standard 140.

Additionally, suppliers should also note that:

- Agency information must not be provided to any third party to 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 will be revoked whenever it is not in use.
- Where suppliers are providing technology security services, periodic competency vetting of supplier personnel will be performed by Agencies in line with contractual agreements and SLAs.

## Document Control

| | |
|---|---|
| ID | SACSF/G2.0 |
| Version | V1.0 |
| Classification/DLM | OFFICIAL |
| Compliance | Discretionary |
| Original authorisation date | November 2019 |
| Last approval date | November 2019 |
| Next review date | November 2020 |