

# South Australian Cyber Security Framework

## Executive Guide

---

SACSF/G1.0

Across Government Guideline

### Purpose

This guideline provides an executive overview of the South Australian Cyber Security Framework (SACSF).

### Introduction

The Government of South Australia manages, delivers and owns information technology infrastructure, services and systems on behalf of the citizens of South Australia. Government agencies must protect infrastructure, digital assets and citizen information against cyber threats to ensure public trust and confidence is maintained, and services delivered to the community are reliable and resilient.

The SACSF is a risk-based framework developed to help maintain the confidentiality, integrity and availability of information and systems. A risk-based approach to cyber security management is not one-size-fits-all and gives agencies flexibility to implement approaches that align to their own risk profile.

The SACSF is a Cabinet approved Framework and forms one part of the overarching South Australian Protective Security Policy Framework. It applies to South Australian Government public sector agencies (as defined in section 3(1) of the [Public Sector Act 2009](#)) and to any other person or organisation that is generally subject to the discretion of a Minister or the Crown.

The SACSF has a range of supporting standards, guidelines and templates to help agencies implement a cyber security program.

### Responsibilities of the agency chief executive

As specified in Premier and Cabinet Circular 30 (PC030), the agency Chief Executive (or equivalent accountable authority responsible for the agency's operations) is responsible for ensuring their agency complies with the South Australian Protective Security Framework (SAPSF), which includes the SACSF. The SACSF is a subordinate document to PC030 and the SAPSF, and includes specific responsibilities for the Chief Executive, including:

- defining the agency's cyber security risk appetite.
- approving the agency's SACSF tier level.
- embedding the cyber security work program into their agency and assigning suitable and sufficient cyber security resources to the work program.
- reviewing and approving the annual SACSF attestation.

## The framework approach

The SACSf includes an implementation approach and 4 core principles:

**Implementation approach:** Guidance on the stages and activities recommended to support an agency cyber security program to deliver an SACSf implementation.

**Governance:** Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.

**Information:** Maintain the confidentiality, integrity and availability of all agency information and systems.

**Personnel:** Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.

**Physical:** Provide a safe and secure physical environment for people, information and assets.

Each principle has a set of underlying policies. The Framework has 18 policies in total that all agencies must address as part of their cyber security program.

To provide agencies with guidance on how they should meet the requirements of a specific policy, the SACSf includes a guided tiering system. Agencies are required to select a tier based on their risk profile, size, complexity, and criticality of their services and can then refer to the SACSf policy requirements to see the types of security controls that should be considered to address the policy.

The tiering model supports a risk-based approach for cyber security management. The tiering is designed to provide agencies with guidance that is tailored to their size, complexity, or criticality. As the tier level increases, so does the level of complexity of the security requirements commensurate with the agency's level of risk.

## Annual reporting and attestation

It is a requirement of the SACSf that agencies provide an annual attestation of their alignment to the framework. Attestations are collated by the Department of Treasury and Finance into a report submitted to Senior Leadership Committee and Cabinet.

The attestation provides an opportunity for agencies to review their security performance in line with their strategic objectives and security goals, as well as providing assurance that agencies are progressing towards the overall security outcomes of SA Government. Insights gained from the SACSf attestation inform SA Government strategies to mitigate cyber security risks to government information and services.

## Guidance and assistance

The SACSf is supported by a suite of documentation, guidance and templates to assist agencies in its implementation, aligned with their existing risk management processes. Visit [www.security.sa.gov.au](http://www.security.sa.gov.au).

Agencies can also seek advice on SACSf implementation, and assistance with cyber security program establishment and improvement, from the Office of the Chief Information Officer. For more information contact the team at [cybersecurity@sa.gov.au](mailto:cybersecurity@sa.gov.au).

## 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

Agencies should contact their agency IT Security Adviser for assistance.

- [South Australian Cyber Security Framework](#)
- [South Australian Protective Security Framework](#)
- [Premier and Cabinet Circular 30 – Protective Security in the Government of South Australia](#)

## Document Control

|                           |                                         |                  |           |
|---------------------------|-----------------------------------------|------------------|-----------|
| Approved by               | CIO Steering Committee                  | Version          | 1.2       |
| Approved date             | 18 June 2025                            | Next review date | June 2027 |
| Original date of approval | November 2019                           | Compliance       | Optional  |
| Contact                   | Office of the Chief Information Officer |                  |           |
| Contact email             | cybersecurity@sa.gov.au                 |                  |           |

### 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, 2025.