SACSF/G1.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

South Australian Cyber Security Framework Executive Guide

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 Protective Security Policy Framework and applies to:

- South Australian Government public sector agencies
- suppliers to the South Australian Government
- non-government personnel who provide services to government agencies.

The SACSF has a range of supporting guidelines and templates to help agencies with implementing a cyber security program in their agency.

Responsibilities of the agency chief executive

As specified in Premier and Cabinet Circular 30 (PC030), the agency Chief Executive is accountable for the security of their agency. The SACSF is a subordinate document to PC030, 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 cyber security attestation.

The framework approach

The SACSF has 4 core principles:

1. **Governance:** Manage security risks and support a positive security culture. Make sure there are clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.
2. **Information:** Maintain the confidentiality, integrity and availability of all agency information and systems.
3. **Personnel:** Make sure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.
4. **Physical:** Provide a safe and secure physical environment for people, information and assets.

Each principle has a set of underlying policies that agencies must consider as part of their approach to managing cyber security.

The Framework has 21 policies in total that agencies must address as part of their cyber security program. Each policy is a wide-ranging statement that agencies must consider, however, the precise approach adopted to comply with the policy will ultimately vary. Agencies have the flexibility to choose the way they address the policy in accordance with their risk profile.

Guidance and assistance

In order to provide agencies with guidance on how they could 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 organisation and can then refer to the SACSF tiering expectations to see the types of security controls that could be considered to address the policy. The tiering expectations are guidance only and are not a compliance checklist that agencies must follow.

The tiering model does not replace the risk-based approach for cyber security management. The tiering is simply designed to provide agencies with guidance that is slightly more tailored to their size, complexity or criticality. This should help less resourced or mature agencies understand the types of approaches they can consider in complying with government cyber security policy.

Annual reporting and attestation

As part of the SACSF, each agency will provide an annual attestation which will be collated by the Department of the Premier and Cabinet with a report submitted for consideration by Senior Management Council and Cabinet. The attestation will provide a high-level overview of how an agency is aligning to the requirements of the SACSF, and how it plans to continue to maintain and meet those requirements. The whole of government report will be de-identified with agencies compared against others of a similar tier.

References, links and additional information

Agencies should contact their agency IT Security Adviser for assistance.

For copies of the SACSF, and all associated guidance and templates, please visit security.sa.gov.au.

Document Control

ID	SACSF\G1.0
Version	V1.0
Classification/DLM	OFFICIAL
Compliance	Guidance
Original authorisation date	November 2019
Last approval date	November 2019
Next review date	November 2020