Premier and Cabinet Circular

PC 030 – PROTECTIVE SECURITY IN THE GOVERNMENT OF SOUTH AUSTRALIA

Effective from September 2023

Contents

Purpose statement 3
Context 3
Authority and accountability 3
Application 4
South Australian Protective Security Framework 4
Principles 4
Security Outcomes 5
South Australian Cyber Security Framework 5
Agency-specific policies and procedures 5
Relationship with PC012 – Information Privacy Principles (IPPS) Instruction 5
Security classified information and assets 6
Commonwealth *Protective Security Policy Framework* 6
Exemptions 6
Monitoring and compliance 6
Distribution and publication 7
Document Control 7
For more information 7

Purpose statement

Protective security comprises the policies and procedures to protect people, information and assets from compromise[1] or harm.

This circular establishes and authorises:

- the overarching policy principles
- the South Australian Protective Security Framework (SAPSF) and Cyber Security Framework
- policy requirements and guidance for South Australian public sector agencies to protect their people, information and assets.

Context

The Government of South Australia and its agencies have a responsibility to implement effective protective security measures which maintain the safety, integrity and viability of its people (including those who come into contact with the government and its services), its information and its assets.

These measures should adapt to the rapidly changing risks and threat environment and help ensure government delivers efficient and effective services. Cyber security forms part of the broader protective security environment.

While all agencies have different requirements and risks, each government agency has a role to play in protecting our people, places and information.

Authority and accountability

The Security, Emergency & Recovery Management (SERM) team in DPC is responsible for administering the SAPSF and coordinating whole of government reporting requirements. Any amendments, revisions or queries should be directed to sapsf@sa.gov.au.

The Cyber Security team in Office of the Chief Information Officer (OCIO), DPC is responsible for administration of the SACSF. Any amendments, revisions or queries should be directed to cybersecurityOCIO@sa.gov.au.

The Accountable Authority[2] of each agency is responsible for ensuring their agency complies with the directions of the circular and the SAPSF, including implementing and funding risk-informed arrangements, maintaining a plan to improve protective security maturity and reporting on progress.

The CE DPC has the authority to approve updates to the framework and supporting documents, such as guidelines, checklists and reporting templates, where the overall policy intent does not change. Significant changes, including changes to core and supporting requirements, must be approved by Senior Leadership Committee prior to submission to Cabinet.

[1] Compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification, and unauthorised disclosure

[2] the person or group of persons responsible for, and with control over, the agency's operations (e.g. Chief Executive, Commissioner)

Significant changes, including changes to core and supporting requirements, must be approved by Senior Leadership Committee prior to submission to Cabinet.

Application

This circular applies to all South Australian 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 direction of a Minister of the Crown; all of which are referred to in this policy as "Agencies".

South Australian Protective Security Framework

The SAPSF outlines core responsibilities and requirements for agencies across four protective security domains: governance (GOVSEC), information[3] (INFOSEC), personnel (PERSEC) and physical (PHYSEC) security.

The SAPSF is a principled, risk-based policy framework created to achieve consistent and effective security outcomes across the South Australian public sector. The framework:

- acknowledges there is no 'one-size-fits-all' approach to security and empowers agencies to identify and manage their individual security risks in line with their risk appetite and strategic objectives
- promotes effective management of security through sound risk-management practices
- supports agencies to develop a cycle of continuous improvement around a strong security culture
- sets one security outcome for each domain, and through a series of 13 policies, establishes core requirements and supporting requirements designed to achieve these outcomes, and
- aligns with both national and international standards, while incorporating relevant legislation, policy and risk-profiles from across South Australia

Each policy consists of one core (mandatory) requirement and a varying number of supporting requirements and is accompanied by guidance that draws upon both national and international standards for protective security. Polices, guidance and supporting material is available to agencies via www.security.sa.gov.au.

Principles

There are five principles that form the foundation of the SAPSF covering the breadth of responsibilities and that apply all areas of protective security:

i. Security is a shared responsibility of government, its agencies and its employees
ii. Every agency must understand what it needs to protect
iii. A robust, risk management approach to security enables effective and proportionate treatment of risk to protect information, people and assets
iv. Strong governance ensures protective security is reflected in agency planning

[3] INFOSEC includes Information Communication Technology (ICT). The SAPSF requires that agencies implement the South Australian Cyber Security Framework to maintain robust ICT and cyber security.

v. A positive security culture empowers personal accountability, promotes ownership and management of risk and supports continuous improvement

Security Outcomes

Each protective security domain has one security outcome, which the policies and requirements are designed to achieve.

Governance	Information	Personnel	Physical
Each agency identifies and manages security risks while establishing and maintaining a positive security culture, and a cycle of continuous improvement.	Each agency maintains the confidentiality, integrity and availability of all official information	Each agency ensures its employees and all contractors are suitable to access South Australian government resources, and meet the required standards of integrity and honesty	Each agency provides a safe and secure physical environment for their people, information and assets

South Australian Cyber Security Framework

The South Australian Cyber Security Framework (SACSF) is the whole of South Australian Government cyber security policy framework, and forms part of the SAPSF.

The SACSF directs and guides agencies through an approach for establishing, implementing, maintaining and continually improving their cyber security posture.

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 supports agencies to adopt a flexible approach to implementing a program that aligns to their own risk profile, recognising that one size does not fit all.

The Framework consists of 21 policy statements that agencies must address as part of their cyber security program. Each policy statement defines cyber security expectations that agencies are required to consider. The precise approach agencies adopt to achieve each policy will vary.

The SACSF and supporting guidelines are available via www.security.sa.gov.au.

Agency-specific policies and procedures

Each agency must have appropriate protective security policies and procedures in place to implement the requirements of the SAPSF and SACSF.

Relationship with PC012 – Information Privacy Principles (IPPS) Instruction

Premier's Circular 012 – Information Privacy Principles (IPPS) Instruction (PC012) establishes principles that agencies must implement, maintain and observe for all personal information they hold and are responsible for.

No directive of PC030 obfuscates or overrides a responsible agency's obligations under PC012 but may assist in delivering the outcomes of PC012.

Security classified information and assets

Security classified information or assets are those classified **PROTECTED** or higher under the South Australian Information Classification System. They have strict access, handling, dissemination and storage requirements due to the sensitivity (e.g. information) or function (e.g. ICT systems) they perform. Requirements include the need for personnel to hold the correct level of security clearance, ICT system compliance and correct physical storage.

Although the SAPSF promotes a risk-based approach to security, agencies **must** comply with all requirements around the creating, handling, disseminating and storing security classified information or assets.

Commonwealth *Protective Security Policy Framework*

The SAPSF has been developed to be consistent with the Commonwealth Government's *Protective Security Policy Framework* (PSPF). While the PSPF is applicable only to all non-corporate Commonwealth Government entities for the protection of their people, information and assets, all Australian jurisdictions **must** comply with the PSPF when handling, accessing or sharing Commonwealth Government information or resources.

Exemptions

Any exemptions to all or part of this circular, including the SAPSF or the SACSF may only be approved by Cabinet.

The Accountable Authority of the agency seeking an exemption must ensure the application:

i. is in writing
ii. states the reasons why the exemption(s) is necessary
iii. specifies the proposed alternative policies, procedures or controls that will be adopted by the agency
iv. explains how the proposed alternative will ensure that protective security is undertaken in a manner that is consistent with all policy requirements.

The SAPSF team must be notified of any exemption requests via SAPSF@sa.gov.au.

Monitoring and compliance

Under the SAPSF and SACSF, agencies are required to submit annual security attestations to provide a level of assurance and demonstrate its level of confidence that it is achieving the overall security outcomes of the South Australian Government. The attestations provide a mechanism for each agency to demonstrate how they are applying the requirements of the SAPSF and SACSF and their effectiveness, and identify their individual risk environment, appetite and tolerance. The outcomes of these processes inform reporting to the Senior Leadership Committee and Cabinet to help guide and inform decision-making.

Any queries should be directed to:

- sapsf@sa.gov.au for the SAPSF
- cybersecurityOCIO@sa.gov.au for the SACSF.

Distribution and publication

The circular will be published on the DPC website and all Chief Executives will be notified when the circular is published or updated.

Document Control

Review number: 2.0
Review date: September 2023

Date of approval: 18 May 2020
Next review date: April 2026

For more information

Security, Emergency and Recovery Management, Department of the Premier and Cabinet

E: sapsf@sa.gov.au
cybersecurityOCIO@sa.gov.au

W: security.sa.gov.au