Premier and Cabinet Circular

PC 030 – PROTECTIVE SECURITY IN THE GOVERNMENT OF SOUTH AUSTRALIA

Effective from July 2020

Contents

Introduction 3
Purpose 3
Authority 3
Applicability 3
Administration 3
Relationship with PC012 – Information Privacy Principles (IPPS) Instruction 4
South Australian Protective Security Framework 4
Guidance and support material 4
Agency-specific policies and procedures 4
Security classified information and assets 5
Commonwealth *Protective Security Policy Framework* 5
South Australian *Protective Security Policy* 5
Document Control 5
For more information 5

Introduction

1. Protective security comprises the policies and procedures to protect people, information and assets from compromise[1] or harm.
2. The Government of South Australia and its agencies have a responsibility to implement effective protective security policies 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, while continuing to deliver efficient and effective services.
3. This circular outlines the strategic decision, approved by Cabinet, for a whole-of-government approach to protective security by adopting the South Australian Protective Security Framework (SAPSF) as the protective security policy requirements for the Government of South Australia.

Purpose

4. To provide each South Australian public sector agency with policy and guidance to protect its people, information and assets.

Authority

5. Premier and Cabinet Circulars are issued by Cabinet and used to establish whole-of-government policy, including instructions or requirements for agencies to take specific action in the implementation of those policies.

Applicability

6. 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”.
7. The accountable authority[2] of each agency is responsible for ensuring their agency’s compliance with the directions of this circular.

Administration

8. Cabinet Office in the Department of the Premier and Cabinet (DPC) is responsible for the administration of Premier’s Circulars. Any agency seeking amendment or revision of this circular must consult with Cabinet Office via DPCCabinetOffice@sa.gov.au.
9. Security and Emergency Management (SEM) team in DPC is responsible for administration of the SAPSF. Any amendments, revisions or queries should be directed to sapsf@sa.gov.au.

[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)

Relationship with PC012 – Information Privacy Principles (IPPS) Instruction

10. *Premier's Circular 012 – Information Privacy Principles (IPPS) Instruction* (PC012) states that the principal officer (accountable authority) must ensure the principles of the IPPS are implemented, maintained and observed for and in respect of all personal information for which her or his agency is responsible.
11. No directive of PC030 obfuscates or overrides a responsible agency's obligations under PC012 but may assist in delivering the outcomes of PC012.

South Australian Protective Security Framework

12. The SAPSF was developed to provide South Australian public sector agencies with protective security policy requirements across the protective security domains of governance (GOVSEC), information[3] (INFOSEC), personnel (PERSEC) and physical (PHYSEC) security.
13. The SAPSF is a principled, risk-based policy framework created to achieve consistent and effective security outcomes across the South Australian public sector. The SAPSF 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.
14. The SAPSF promotes effective management of security through sound risk-management practices, which support agencies to develop a cycle of continuous improvement around a strong security culture.
15. Each policy consists of one core requirement and a varying number of supporting requirements designed to achieve a stated security outcome. There is one security outcome for each security domain.
16. All polices, guidance and supporting material of the SAPSF is available to agencies via www.security.sa.gov.au.

Guidance and support material

17. Each policy is accompanied by guidance to assist agencies to implement the core and supporting requirements of the SAPSF. The guidance has been developed to be consistent with both national and international standards, while incorporating relevant legislation, policy and risk-profiles from across South Australia. Where applicable, supporting documentation is also referenced or provided.
18. All agencies should reference the guidance material when applying each requirement of the SAPSF.

Agency-specific policies and procedures

19. It is the responsibility of the accountable authority to ensure their agency has the appropriate protective security policies and procedures in place to implement the requirements of the SAPSF.

[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.

Security classified information and assets

20. Security classified information or assets are those classified **PROTECTED** or higher under the South Australian Information Classification System. Information or assets that are security classified 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.
21. While a risk-based approach to security is promoted throughout the SAPSF, agencies **must** comply with all requirements around the creation, handling, dissemination and storage of security classified information or assets.

Commonwealth *Protective Security Policy Framework*

22. 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.

South Australian *Protective Security Policy*

23. The policies of the SAPSF are complementary to the South Australian Government's *Protective Security Policy* (PSP). The PSP outlines the specific requirement that protective security services to South Australian Government assets designated as Critical Infrastructure of High-Risk (CI-HR) be provided by South Australia Police's Police Security Services Branch.
24. No directive of the SAPSF obfuscates or overrides a responsible agency's obligations regarding sites designated as CI-HR, but implementation of the SAPSF may assist in increasing site security.

Document Control

Review number: 1.0
Review date:

Date of approval: 18 May 2020
Next review date:

For more information

Security and Emergency Management,
Department of the Premier and Cabinet
T: 0447180915

E: sapsf@sa.gov.au

W: dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars