



# South Australian Protective Security Framework (SAPSF)

## Executive Guide

A framework for the protection of  
information, people and assets in the  
South Australian Public Sector

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

### Introduction

The Government of South Australia has a responsibility to protect its people, information and assets. The South Australian Protective Security Framework (SAPSF) provides all government entities with the requirements and guidance required to implement and maintain protective security processes and procedures that identify and manage risk, promote continuous improvement to security capability and maturity, and foster a positive security culture throughout the South Australian public sector.

The SAPSF consists of 13 Core Requirements, which are based on existing national and international standards, to assist all agencies manage individual and collective protective security risks.

The SAPSF is a risk-based framework designed to empower agencies to identify and manage the most significant risks to South Australian Government business.

The requirements of the SAPSF have been developed to integrate with existing practices at a state, jurisdictional and Commonwealth level, including with the Commonwealth Protective Security Policy Framework (PSPF).

# SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

## Contents

<b>INTRODUCTION</b> .....	2
<b>TERMINOLOGY</b> .....	4
<b>PURPOSE</b> .....	4
<b>AUTHORITY/DIRECTIVE</b> .....	4
<b>APPLICABILITY</b> .....	4
<b>SCOPE</b> .....	4
RELATIONSHIP WITH PC012 - INFORMATION PRIVACY PRINCIPLES (IPPS) INSTRUCTION.....	5
SOUTH AUSTRALIAN PROTECTIVE SECURITY POLICY .....	5
<b>PROTECTIVE SECURITY FRAMEWORK STRUCTURE</b> .....	5
PRINCIPLES.....	5
OUTCOMES .....	7
POLICIES.....	7
GUIDANCE AND SUPPORT MATERIAL.....	7
AGENCY-SPECIFIC POLICIES AND PROCEDURES .....	7
<b>GOVSEC1: SECURITY GOVERNANCE</b> .....	8
<b>GOVSEC2: SECURITY PLANNING</b> .....	9
<b>GOVSEC3: SECURITY MONITORING</b> .....	10
<b>GOVSEC4: ANNUAL SECURITY ATTESTATION</b> .....	11
<b>GOVSEC5: MANAGING THE SECURITY OF CONTRACTORS AND SERVICE PROVIDERS</b> .....	12
<b>GOVSEC6: SECURITY GOVERNANCE FOR INTERNATIONAL SHARING</b> .....	13
<b>INFOSEC1: PROTECTING OFFICIAL INFORMATION</b> .....	14
<b>INFOSEC2: ACCESSING OFFICIAL INFORMATION</b> .....	15
<b>INFOSEC3: ROBUST ICT AND CYBER SECURITY</b> .....	16
<b>PERSEC1: RECRUITING EMPLOYEES</b> .....	17
<b>PERSEC2: MAINTAINING EMPLOYEE SUITABILITY</b> .....	18
<b>PERSEC3: EMPLOYEE SEPARATION</b> .....	19
<b>PHYSEC1: PHYSICAL SECURITY</b> .....	20
<b>DEFINITIONS</b> .....	21
<b>ACRONYMS</b> .....	23
<b>RELATED DOCUMENTS</b> .....	24

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

## Terminology

Term	Meaning
<b>MUST</b>	Use of the word <b>must</b> (or <b>required</b> or <b>responsible for</b> ) indicates a requirement or action of the policy to which all agencies must adhere or undertake
<b>MUST NOT</b>	Use of the words <b>must not</b> indicates an action prohibited by this policy
<b>SHOULD</b>	Use of the word <b>should</b> (or <b>recommended</b> ) indicates an action that agencies ought to undertake, unless prevented by legitimate circumstances or justification
<b>SHOULD NOT</b>	Use of the words <b>should not</b> (or <b>not recommended</b> ) indicates an action which agencies should avoid, unless legitimate circumstances prevent another course of action being taken
<b>MAY</b>	Use of the word <b>may</b> indicates an action which is completely optional, but may be provided as a suggestion or considered best practice

## Purpose

1. To provide each South Australian public sector agency<sup>1</sup> with the policy and guidance by which to protect its information, people and assets.

## Authority/Directive

2. The South Australian Protective Security Framework (SAPSF) has been adopted by Cabinet under Premier and Cabinet Circular 030 (PC030): *Protective Security in the Government of South Australia*, as the protective security policy framework for the Government of South Australia.

## Applicability

3. The SAPSF 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”.
4. Non-government organisations that access sensitive or security classified government information **must** enter into a deed or agreement to apply relevant parts of the SAPSF for the information or resources they have access to.
5. Contractors and service providers are also **responsible for** implementing the security requirements of the SAPSF, consistent with the terms and conditions of contracts or service agreements to which they are a signatory.

## Scope

6. The SAPSF provides South Australian public sector agencies with protective security policy requirements across all the protective security domains (governance, information (including ICT), personnel and physical) to assist each agency to identify, manage and mitigate security risks accordingly.
7. Where South Australian agencies handle information owned by the Commonwealth, or pertaining to matters in the national interest, that information must be treated in accordance with requirements as set out under the *Commonwealth Protective Security Policy Framework* (PSPF). These requirements are mandatory and supersede any obligations of the SAPSF.

<sup>1</sup> See [Applicability](#)

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

8. The SAPSF is has been developed to be consistent with relevant South Australian legislation. Where relevant legislation mandates a lower standard than the SAPSF, agencies are encouraged to meet the higher standard of the SAPSF.

### Relationship with PC012 - Information Privacy Principles (IPPS) Instruction

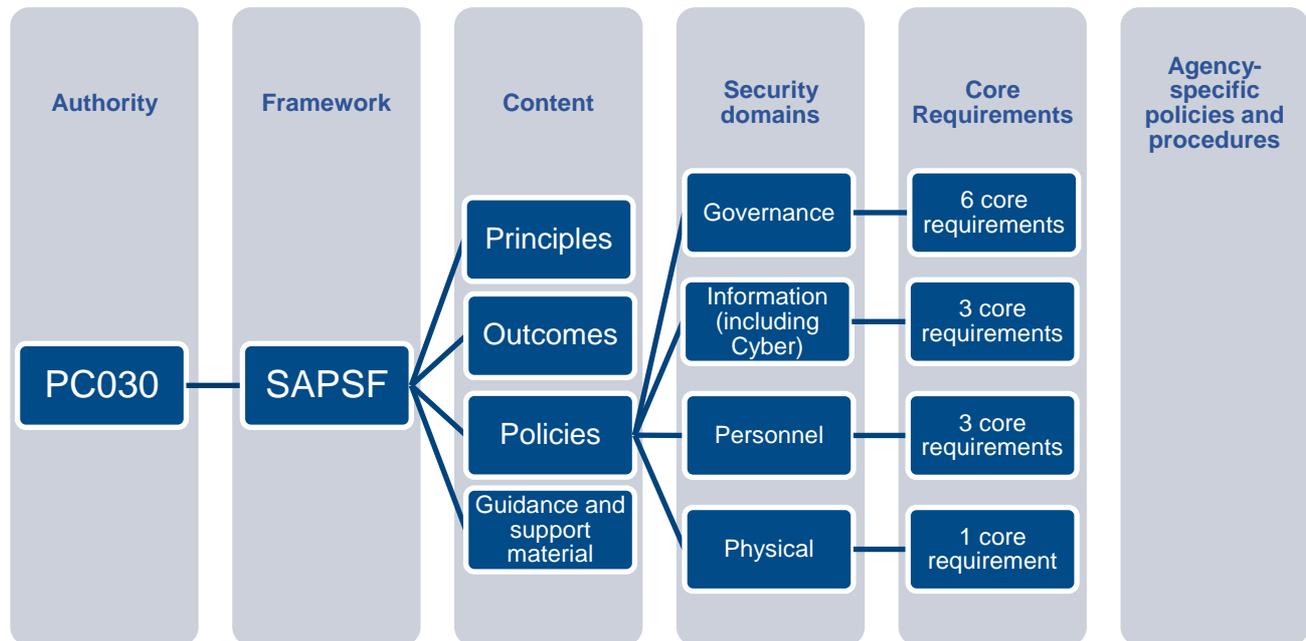
9. [Premier’s Circular 012 – Information Privacy Principles \(IPPS\) Instruction](#) (PC012) states that the principal officer (accountable authority) must ensure the principles of the IPPS are implemented, maintained and observed for and in respect of all personal information for which her or his agency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

### South Australian Protective Security Policy

11. The policies of the SAPSF are complementary to the South Australian Government’s [Protective Security Policy](#) (PSP), which outlines the requirement that protective security services to South Australian Government assets designated as Critical Infrastructure of High-Risk (CI-HR) be provided by SAPOL’s Police Security Services Branch (PSSB). In addition, the PSP also requires all agencies to obtain all security monitoring services from PSSB.
12. No directive of the SAPSF obfuscates or overrides a responsible agency’s obligations regarding sites designated as CI-HR, but implementation of the policies may assist in increasing the security of the site.

### Protective Security Framework Structure

13. The structure of the protective security framework is as follows:



### Principles

14. There are five (5) principles that form the foundation of the SAPSF. They cover the breadth of responsibilities under the SAPSF, and apply to all areas of protective security. It is expected the principles will guide decision making within agencies to achieve a cycle of continuous improvement.

- I. **SECURITY IS A SHARED RESPONSIBILITY OF GOVERNMENT, ITS AGENCIES AND ITS EMPLOYEES**

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

15. A protective security framework is only as good as its weakest point. The South Australian community places a high-degree of trust and expectation in public sector agencies to protect its information, people and assets while providing efficient and effective services.
16. Official information and resources in the public sector have an inherent value that must be recognised, and it is the responsibility the South Australian public sector agencies to value the information and resources they hold and identify and mitigate any risks in order to keep them safe from compromise or damage.

### **II. EVERY AGENCY MUST UNDERSTAND WHAT IT NEEDS TO PROTECT**

17. Information, people and assets are valuable resources to the South Australian Government.
18. Agencies have a responsibility to apply the right protections to their most valuable resources in line with the identified risk tolerance of the agency.
19. The SAPSF provides the tools and guidance to enable agencies to effectively assess their most important resources, and determine how to protect them.

### **III. A ROBUST, RISK MANAGEMENT APPROACH TO SECURITY ENABLES EFFECTIVE AND PROPORTIONATE TREATMENT OF RISK TO PROTECT INFORMATION, PEOPLE AND ASSETS**

20. A robust risk-management approach supports the perpetual protection of information, people and assets within public sector agencies by enabling existing risks to be monitored and treated while ensuring new risks are identified, assessed and prioritised within the same context.
21. To support this principle, accountable authorities will be required to develop, implement and maintain an agency security plan that utilises effective risk-management practices, enabling agencies to effectively diagnose, assess and treat risks in a manner proportionate to their operational context.

### **IV. STRONG GOVERNANCE ENSURES PROTECTIVE SECURITY IS REFLECTED IN AGENCY PLANNING**

22. Security **must** be a consideration across all aspects of service delivery in the public sector, which relies on strong leadership and ownership of risk across an agency's protective security governance arrangements.
23. Governance arrangements that appropriately reflect the size, requirements and risk of an agency have an enormous impact upon the success of a protective security system and the efficient and effective delivery of government services.
24. Accountability for the security of an agency's information, people and assets rests with the accountable authority<sup>2</sup>, whose responsibility it is to implement strong governance to support this principle.

### **V. A POSITIVE SECURITY CULTURE EMPOWERS PERSONAL ACCOUNTABILITY, PROMOTES OWNERSHIP AND MANAGEMENT OF RISK AND SUPPORTS CONTINUOUS IMPROVEMENT**

25. A positive security culture is the product of effective security leadership in combination with acceptance of security as a shared responsibility of government, its agencies and its employees.
26. The attitudes and behaviours of individuals contribute to building, but can also quickly erode, a strong organisational security culture.
27. The SAPSF aims to embed security within all elements of an agency's business by changing the narrative of security as something that needs to be applied and instead as something that inherently exists within an agency's systems and practices.

---

<sup>2</sup> the person or group of persons responsible for, and with control over, the agency's operations

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

28. The application of security-conscious policies and behaviours can be a powerful business enabler that reduces the significance and frequency of risk and helps to deliver more efficient, more secure government services.

### Outcomes

29. These are high-level statements identifying the desired end-state of the SAPSF requirements that the Government seeks to achieve. There is one outcome for each of the four security domains: governance (GOVSEC), information (INFOSEC), personnel (PERSEC) and physical (PHYSEC).

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

### Policies

30. The SAPSF is made up of 13 policies in total across the four protective security domains (6 GOVSEC, 3 INFOSEC, 3 PERSEC and 1 PHYSEC policy). Each policy contains one high-level, core (mandatory) requirement and a varying number of supporting requirements.

### Guidance and support material

31. Each policy is accompanied by guidance to assist agencies to implement the core and supporting requirements of the SAPSF. The guidance draws upon both national and international standards for protective security, while incorporating relevant legislation, policy and risk-profiles from across South Australia. Where applicable, supporting documentation is also referenced or provided.

### Agency-specific policies and procedures

32. The policies and procedures within agencies to implement the requirements of the SAPSF are outside the scope of the SAPSF. The responsibility for implementing effective security measures rests with the accountable authority of each agency. It is their responsibility to ensure their agency is managing its security risks in line with the requirements of the SAPSF, and the risk profile and appetite of the agency.

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# GOVSEC1: Security governance

## Purpose

1. This policy describes how an agency's accountable authority can establish effective security governance to protect their agency's people, information and assets. An effective governance structure ensures employees with the appropriate knowledge and position are empowered and resourced to maintain agency security.

## Core Requirement 1

***The accountable authority must establish the right security governance for the agency***

## Supporting Requirements

2. To ensure an agency establishes the right security governance, the accountable authority **must**:
  - I. be responsible for protective security within the agency, including:
    - a. putting in place protective security arrangements that implement the core and supporting requirements of the SAPSF
  - II. determine and manage the agency's security risks
  - III. appoint an Agency Security Executive (ASE) to be responsible for directing protective security and empower them to make decisions about the agency's security, including:
    - a. appointing security advisors (ASAs & ITSAs) to advise on, and support delivery of, security outcomes, including sound information and communication technology (ICT) policies and procedures
  - IV. develop practices and procedures that deliver the security plan
  - V. detect, respond, investigate and report security incidents
  - VI. be aware of and meet all security policy or legislative requirements
  - VII. provide and maintain security awareness training for all employees and service providers
  - VIII. establish, maintain and monitor a central email address for all security matters across all protective security domains, including ICT.

## Guidance

3. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# GOVSEC2: Security planning

## Purpose

1. Good security planning will assist agencies to identify and manage security risks while maintaining the continuous delivery of efficient and effective government services. This policy describes how agencies can effectively manage security risks through planning and embedding security into risk management practices and procedures.
2. Security planning through risk management processes enables agencies to prioritise the most critical risks, set protective security targets, adjust objectives based on changes to the risk environment, improve agency resilience to threats and overall protective security maturity.

## Core Requirement 2

### *Maintain a security plan<sup>3</sup> to manage security risks*

## Supporting Requirements

3. To establish a security plan that manages security risks, agencies **must**:
  - I. determine the agency's security goals and strategic objectives
  - II. determine the risk tolerance for the agency
  - III. identify the agency's security risks, including shared risks
  - IV. plan and implement treatments to manage agency security risks
  - V. identify a risk manager to be responsible for each security risk, or category of security risk
  - VI. document any decisions to deviate from the security plan, including justifications and alternative treatments implemented
  - VII. review the security plan (and any supporting security plans) at least every two years for:
    - a. the adequacy of existing security arrangements and risk treatments
    - b. significant changes to the risk environment or tolerance.

## Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>3</sup> Where a single security plan is not practicable due to the agency's size or complexity of business, the accountable authority **may** approve a single, strategic-level overarching security plan that addresses the core requirements of the SAPSF, which is then supported by other more details plans (supporting security plans).

# GOVSEC3: Security monitoring

## Purpose

1. Security maturity is a meaningful way of measuring an agency's overall security capability in line with the risk environment and the agency's risk tolerances. Maturity recognises the inherent differences between agencies, functions, risk environments and security risks, and acknowledges the journey agencies may need to take to achieve their security goals and objectives, while helping to identify areas for improvement.
2. This policy ensures that agencies develop and implement processes to routinely monitor and assess their security maturity in line with the security goals of their security plan. An agency's security maturity includes the ability to actively respond to changes in the agency's security risk environment, including to new and emerging threats or vulnerabilities, to ensure the ongoing protection of its people, information and assets.

## Core Requirement 3

### *Monitor security maturity against the security plan*

## Supporting Requirements

3. To monitor security maturity against the security plan, agencies **must**:
  - I. seek, identify and document evidence of the agency's security maturity
  - II. assess progress to achieving the security goals and maturity targets of the security plan
  - III. amend the security plan in accordance with changes to the risks, threats, vulnerabilities or criticalities of the agency.

## Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# GOVSEC4: Annual security attestation

## Purpose

1. The policies of the SAPSF are designed to ensure the security information, people and assets within the South Australian Government. However, how each agency applies the policies and their effectiveness depends significantly on the risks identified, the risk environment an agency operates in, and each agency's individual risk appetite and tolerance.
2. The annual security attestation, signed by an agency's accountable authority, provides a mechanism for each agency 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, while also identifying broader protective security risks or challenges.

## Core Requirement 4

***Provide an annual security attestation to the Department of the Premier and Cabinet on progress against the security plan***

## Supporting Requirements

3. To attest to progress against the security plan, agencies **must**:
  - I. identify progress against the security goals and strategic objectives of the agency's security plan, including:
    - a. justification for any decisions to depart from SAPSF core or supporting requirements
    - b. identify significant challenges or barriers
  - II. assess current security maturity against each security outcome and core requirements of the SAPSF
  - III. identify the key risks to the agency's people, information and assets including:
    - a. new and emerging risks
    - b. risks to other agencies or parties.

## Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

# GOVSEC5: Managing the security of contractors and service providers

## Purpose

1. Security risks can arise through the procurement of goods and services and effective risk management is required to reduce the likelihood and consequence of security issues or incidents.
2. This policy supports the South Australian Government's procurement requirements which detail how agencies procure goods and services. The requirements of this policy seek to ensure security risk is a considered element in all procurement processes.

## Core Requirement 5

***Manage any security risks that arise from the procurement of goods and services***

## Supporting Requirements

3. To ensure any security risks that arise from the procurement of goods and services are managed, agencies **must**:
  - I. identify and mitigate security risks to the agency's people, information and assets generated by the procurement
  - II. ensure relevant security terms and conditions are included in contracts and service agreements that manage identified security risks to the procurement
  - III. manage and monitor:
    - a. security risks for changes or incidents that could affect the procurement, service agreement or security of the agency
    - b. the performance of the contractor (including subcontractors) over the lifetime of the contract
  - IV. implement appropriate security arrangements to manage the completion or termination of a contract or agreement.

## Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# GOVSEC6: Security governance for international sharing

## Purpose

1. From time to time, agencies in South Australia may need to enter official relationships with foreign partners or entities<sup>4</sup>. Security protections are required to ensure that the information or assets are not compromised or exposed to uncontrolled risks.
2. This policy ensures all agencies formalise all partnerships or relationships with foreign partners or agencies through international agreements or arrangements that safeguard the interests, information and assets of both the South Australian and Commonwealth Governments.

Communicating, or making available, security classified information with another country or foreign organisation could be considered espionage under the [Criminal Code](#).

However, specific legislative provisions authorise agencies to share information internationally under arrangements made or directions given by the relevant minister.

## Core Requirement 6

***Ensure adherence to any provisions for the security of people, information and assets contained in international agreements and arrangements to which Australia is a party***

## Supporting Requirements

3. To ensure adherence to security provisions contained in international agreements and arrangements, agencies **must**:
  - I. comply with the core and supporting requirements of the Australian Government Protective Security Policy Framework (PSPF) policy [Security governance for international sharing](#).

## Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>4</sup> A foreign entity includes a foreign government and foreign contractors (meaning any individual or legal entity entering into or bound by a classified contract and includes subcontractors).

# INFOSEC1: Protecting official information

## Purpose

1. This policy ensures all South Australian Government agencies protect their information assets from compromise. It outlines the South Australian Information Classification System (ICS) and associated guidance which all agencies **must** use to protect the confidentiality, integrity and availability of all official information. The requirements of this policy are designed to mitigate against both intentional and accidental threats and reduce the impact on government business.

## Core Requirement 7

### ***Protect the agency's information against compromise<sup>5</sup>***

## Supporting Requirements

2. To protect the agency's information against compromise, agencies **must**:
  - I. determine the appropriate classification and any protections that apply to official information
  - II. set the classification at the lowest reasonable level to protect against compromise to the confidentiality, integrity or availability of all official information
  - III. ensure all *sensitive* and *security classified* information (including emails) are marked with the correct protective markings
  - IV. manage access to information systems by applying the South Australian Recordkeeping Metadata Standard
  - V. ensure all information is handled according to the classification and protective markings assigned to that information
  - VI. seek permission from the information originator to make changes to the classification or protective markings
  - VII. ensure processes for transferring or transmitting sensitive and security classified information deter and detect compromise
  - VIII. ensure sensitive and security classified information is stored securely in an appropriate security container for the approved security zone
  - IX. ensure sensitive and security classified information is disposed of securely
  - X. be responsible for caveated and accountable material.

## Guidance

3. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>5</sup> Information compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification, and unauthorised disclosure

# INFOSEC2: Accessing official information

## Purpose

1. This policy ensures all South Australian Government agencies provide timely, reliable and appropriate access to official information to assist in facilitating efficient and effective delivery of government services. Availability of accurate information aides in the development of new products and services, enhances consumer and business outcomes and assists with decision-making and policy development.

## Core Requirement 8

***Ensure official information is available to those who need it***

## Supporting Requirements

2. To ensure official information is available to those who need it, agencies **must**:
  - I. ensure information is accessed only by personnel with a legitimate need-to-know
  - II. ensure personnel requiring ongoing access to sensitive information have undertaken the appropriate pre-employment screening checks
  - III. ensure personnel requiring ongoing access to security classified information have the appropriate security clearance<sup>6</sup> and meet any additional suitability requirements<sup>7</sup>
  - IV. put in place an agreement or arrangement<sup>8</sup> to enable sensitive or security classified information to be shared with personnel or organisations outside of the South Australian Government
  - V. manage access to information systems by implementing unique user identification, authentication and authorisation practices for each approval of system access
  - VI. ensure temporary access to security classified information is strictly controlled according to the requirements of this policy

## Guidance

3. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>6</sup> Some office holders are not required to hold a security clearance. See **Error! Reference source not found.** for the full list.

<sup>7</sup> Some caveats or codeword information **may** impose additional requirements on the individual *in addition to* the security clearance. Please refer to PSPF policy [Access to information](#) for more detail.

<sup>8</sup> Such as a contract or deed which outlines how the information is to be used and what protections **must** be applied.

# INFOSEC3: Robust ICT and cyber security

## Purpose

1. This policy describes how all South Australian Government agencies can safeguard their information and communication technology (ICT) systems to ensure the confidentiality, integrity and availability of official information. This includes defending against common and emerging cyber threats (e.g. bots, malware, ransomware, spam) and the threat of malicious insiders, while facilitating the continuous delivery of government business.

## Core Requirement 9

***Safeguard ICT systems from compromise to ensure confidentiality, integrity and availability of official information is maintained***

## Supporting Requirements

2. To safeguard ICT systems from compromise to ensure confidentiality, integrity and availability of official information is maintained, agencies **must**:
  - I. apply the appropriate processes and protections as outlined in the [South Australian Cyber Security Framework](#).

## Guidance

3. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# PERSEC1: Recruiting employees

### Purpose

1. This policy assists South Australian Government agencies to recruit eligible and suitable employees by undertaking appropriate and consistent pre-employment screening and vetting processes for all employees.
2. Consistency in recruitment processes ensures a high-level of assurance that employees are fit to occupy their roles and undertake the responsibilities of their positions, including the protection of government information and resources.

### Core Requirement 10

#### *Ensure the suitability of all new employees*

### Supporting Requirements

3. To ensure the suitability of all new employees, agencies **must**:
  - I. ensure all pre-employment checks are conducted in accordance with the South Australian Information Privacy Principles (IPPS) Instruction
  - II. undertake all mandatory pre-employment screening checks, including:
    - a. a Pre-Employment Declaration consistent with the minimum standard issues by the Commissioner for Public Sector Employment
    - b. identity and eligibility checks
    - c. reference checks
    - d. National Police Certificate or other appropriate background screening where required for the role
  - III. any other checks that assist in determining an applicant's suitability to hold the position and access South Australian Government information and resources
  - IV. identify and record all positions requiring a security clearance and the level of clearance required
  - V. ensure people occupying identified positions hold valid security clearances issued by the Australian Government Security Vetting Agency (AGSVA), or another authorised vetting agency

### Guidance

4. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

# PERSEC2: Maintaining employee suitability

## Purpose

1. This policy assists South Australian Government agencies to ensure they maintain a high-level of confidence in their employee's ongoing suitability to access South Australian Government information and resources.
2. Applying this policy helps to ensure that each agency's employees continue to meet all eligibility and suitability requirements established at the point of employment, or commencement in their current position, as well as manage the risk of insider threat.
3. This policy is to be applied in conjunction with South Australian Protective Security Framework (SAPSF) policy *Recruiting employees*.

## Core Requirement 11

### *Ensure the ongoing suitability of all employees*

## Supporting Requirements

4. To ensure the ongoing suitability of all employees, agencies **must**:
  - I. establish processes to maintain confidence that all employees remain suitable to hold their position
  - II. ensure security cleared employees<sup>9</sup> comply with the minimum requirements of their clearance at all times
  - III. share information of security concern with the appropriate authorities.

## Guidance

5. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>9</sup> Including eligibility waivers and conditional security clearance holders

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# PERSEC3: Employee separation

## Purpose

1. This policy sets out how South Australian Government agencies can manage any risks when people stop working for them, including ensuring departing employees maintain the requirement to protect South Australian Government information and resources.
2. In this context, employee separation includes:
  - a. employees leaving an agency, via transfer to another agency, resignation from the public sector or end of contract
  - b. those whose employment has been terminated for any reason<sup>10</sup>
  - c. employees transferring either temporarily or permanently to another state, territory or Commonwealth Government agency
  - d. those taking extended leave<sup>11</sup>.
3. This policy is to be applied in conjunction with SAPSF policies **Recruiting employees** and **Maintaining employee suitability**.

## Core Requirement 12

### ***Securely manage the separation of all employees***

## Supporting Requirements

4. To ensure the secure separation of all employees, agencies **must**:
  - I. remove access to South Australian Government information and resources
  - II. ensure sponsorship of security cleared employees<sup>12</sup> is withdrawn or transferred
  - III. remind separating employees of their ongoing security obligations
  - IV. share information of security concern with the appropriate stakeholders or authorities<sup>13</sup>
  - V. manage any residual risks following the individual's departure.

## Guidance

5. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>10</sup> For employees covered by the *Public Sector Act 2009*, section 54 outlines potential grounds for termination. Additionally, some agencies **may** have other applicable legislation outlining termination provisions.

<sup>11</sup> This policy does not define a period of time for where 'extended leave' applies. See Extended leave for more guidance.

<sup>12</sup> Including eligibility waivers and conditional security clearance holders

<sup>13</sup> Depending on the level of concern this **may** include the ASE, clearance sponsor, authorised vetting agency or the Australian Security Intelligence Organisation (ASIO)

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

# PHYSEC1: Physical security

## Purpose

1. Agencies have a responsibility to ensure their people, information and assets (resources) are protected from harm, including compromise. This policy ensures agencies take the necessary steps to minimise physical security risks to an agency's resources, while also ensuring agencies incorporate protective security requirements into the planning, selection, design and modification of their facilities.

## Core Requirement 13

***Implement physical security measures that minimise the risk of harm or compromise to people, information and physical assets***

## Supporting Requirements

2. To ensure physical security measures minimise the risk of harm or compromise to people, information and physical assets, agencies **must**:
  - I. identify and categorise the agency's resources that require a level of physical protection
  - II. incorporate protective security in the process of planning, selecting, designing and modifying agency facilities
  - III. implement physical security measures proportionate to the assessed business impact of harm or compromise to agency resources, including:
    - a. zoning all work areas
    - b. applying all required individual control elements
    - c. ICT equipment and facilities
  - IV. certify and accredit all security zones
    - a. ensuring areas where sensitive or security classified information is used, transmitted, stored or discussed are certified in accordance with the applicable ASIO Technical Notes<sup>14</sup>
  - V. dispose of physical assets securely
  - VI. manage security risks associated with working away from the office

## Guidance

3. The guidance material for this policy is available via [www.security.sa.gov.au](http://www.security.sa.gov.au).

---

<sup>14</sup> ASIO Technical Notes are available via [GovTeams](#). Users will be required to [register](#) and request access to the Protective Security Policy community.

# SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

## Definitions

### Relevant terms and definitions

Term	Definition
<b>accountable authority</b>	the person or group of persons responsible for, and with control over, the agency's operations
<b>agency</b>	as per the definition of <i>public sector agency</i> (as defined in section 3(1) of the <i>Public Sector Act 2009</i> ) 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".
<b>agreement or arrangement</b>	a document, such as a contract or deed, which outlines how the information is to be used and what protections must be applied
<b>authorised vetting agency</b>	either the Australian Government Security Vetting Agency or another agency that has been authorised by AGSVA to undertake security vetting for its employees
<b>availability</b>	allowing authorised persons to access information for authorised purposes at the time they need to do so
<b>business impact</b>	the assessed impact upon business (individual, agency or government) operations from compromise of the information
<b>caveat</b>	a warning that the information contained has special protections <i>in addition to</i> those indicated by the classification
<b>classification</b>	an indication of the level of protection information needs to prevent compromise (for example OFFICIAL: Sensitive)
<b>clearance sponsor</b>	refers to the agency or entity who sponsors a security clearance on behalf of the applicant. Security clearances are only valid with a valid sponsor. The Department of the Premier and Cabinet sponsors all SA Government security clearances <sup>15</sup> .
<b>compromise</b>	includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure.
<b>confidentiality</b>	limiting of access to information to authorised persons for approved purposes.
<b>container</b>	physical container (such as a lockable cabinet or safe) used to store official information, most notably for sensitive and security classified information
<b>contract</b>	a formal and legally binding agreement which outlines the terms and conditions for the provision of goods or services by an external entity or third party to a South Australian Government agency (same as <b>service agreement</b> )
<b>contractor</b>	the external or third-party contracted to provide services to an agency (same as <b>service provider</b> and for the purposes of this policy, includes subcontractors)
<b>damage</b>	the resulting effects that compromise of information could be expected to cause (commensurate with 'business impact')

<sup>15</sup> South Australia Police (SAPOL) is an authorised vetting agency and clearance sponsor of SAPOL employees for NV1 and NV2 level security clearances.

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Term	Definition
<b>eligibility</b>	where the individual has the right to work in Australia, either as a citizen, or holding a valid work visa
<b>function</b>	the purpose or role an agency undertakes on behalf of the Government of South Australia
<b>handling</b>	any processes for accessing, transmitting, transferring, storing or disposing of, official information
<b>harm</b>	to cause injury or damage, either physically or psychologically, to another person or group of people
<b>identity</b>	who a person is, or the qualities or details that make them unique from others
<b>insider threat</b>	the risk posed to an agency from deliberate or accidental compromise to information and resources from employees or service providers (including contractors)
<b>integrity</b>	assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid
<b>malicious insider</b>	an employee, former employee, contractor or business associate with legitimate access to an agency system or data, who uses that access to steal or destroy data or sabotage systems. Knowledge of a malicious insider must be reported to the appropriate authorities
<b>official information</b>	all information created, sent and received as part of work of the South Australian Government
<b>originator</b>	agency or individual that initially generated and/or is responsible for the information (also owner)
<b>personnel</b>	all people that an agency employs (including contracted employees)
<b>protection</b>	the steps taken to maintain the confidentiality, integrity and availability of official information, or the safety of people and assets
<b>protective marking</b>	identifies the level of classification and any other handling instructions or protections the information requires
<b>resources</b>	an agency's people, information and assets
<b>risk tolerance</b>	the amount of level of risk an agency is comfortable taking after risk treatments have been applied to achieve and objective or manage a security risk
<b>risk treatment</b>	considered, coordinated and efficient actions and resources that mitigate or lessen the likelihood or negative consequences of a security risk
<b>screening</b>	The processes associated with investigating the background of potential employees to determine their suitability to hold and undertaken the responsibilities of a position
<b>security classified</b>	indicates the information or asset holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to the information or asset must be controlled and accessed by appropriately security cleared staff.
<b>security advisors</b>	employees appointed within an agency to undertake specific responsibilities for security (Agency Security Advisors (ASA), Information Technology Security Advisors ITSA))

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Term	Definition
<b>security domains</b>	the areas to which protective security requirements apply: governance, information, personnel and physical
<b>security maturity</b>	a measure of an agency's security position within its risk environment and risk tolerances, while acknowledging progression toward security outcomes
<b>security plan</b>	how an agency articulates how its security risks have been identified, prioritised and will be managed in line with the agency's objectives
<b>security risk</b>	something that can result in compromise, loss, unavailability or damage to an agency's resources, including causing harm to people
<b>sensitive</b>	indicates information requires <i>some</i> level of protection but is not security classified
<b>separation</b>	the process where employees permanently or temporarily leave their employment with an agency
<b>service agreement</b>	see <b>contract</b>
<b>service provider</b>	see <b>contractor</b>
<b>shared risk</b>	security risks that extend across multiple agencies and/or their premises, that impact the community, industry and international or interstate jurisdictions or partners
<b>stakeholder</b>	a person, group or agency with an interest in the security of an individual or entity
<b>suitability</b>	the combination of eligibility and fit for the role, assessment of integrity and ability to meet the assessment criteria or other requirements
<b>threat</b>	a declared intent to inflict harm on personnel or property
<b>value</b>	the assessed importance of the information based upon the potential consequences of compromise – (including but not limited to, monetary value)
<b>vulnerability</b>	the degree of susceptibility and resilience of an agency to risks and threats
<b>zone</b>	the physical entities and work spaces in which official information is produce, accessed, handled and stored.
<b>zoning</b>	the process for determining the appropriate security zone and implementing required control elements

### Acronyms

Acronym	Words
<b>AGSVA</b>	Australian Government Security Vetting Agency
<b>ASE</b>	Agency Security Executive
<b>ASIO</b>	Australian Security Intelligence Organisation
<b>CI-HR</b>	Critical Infrastructure High-Risk
<b>ICS</b>	Information Classification System

## SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Acronym	Words
ICT	Information Communication Technology
IPPS	Information Privacy Principles Instruction (also see PC012)
ISM	Information Security Manual (Commonwealth)
ISMF	Information Security Management Framework (South Australia)
PC012	Department of the Premier and Cabinet Circular - <b>PC012</b> (see IPPS)
PC030	Premier and Cabinet Circular 030 – Protective Security in the Government of South Australia
PSPF	Protective Security Policy Framework (Commonwealth)
PSSB	Police Security Services Branch
SACSF	South Australian Cyber Security Framework (replacing the ISMF)
SAPOL	South Australia Police
SAPSF	South Australian Protective Security Framework

### Related documents

[South Australian Protective Security Framework](#)

[South Australian Cyber Security Framework \(SACSF\)](#)

[Protective Security Act 2007](#)

[Protective Security Policy](#)

[Department of the Premier and Cabinet Circular - PC012 Information Privacy Principles \(IPPS\) Instruction \(PC012\)](#)

[Protective Security Policy Framework \(Commonwealth\)](#)

[Information Security Manual \(Commonwealth\)](#)

---

### DOCUMENT CONTROL:

Approved by: Jim McDowell

Title: Chief Executive, Department of the Premier and Cabinet

Contact person: James Doherty

Telephone: 0447 180 915

Division: Security and Emergency Management, Intergovernmental and Diplomatic Relations

Date of approval: 20 April 2020

Revision number: 1.0

Date of review: n/a

Next review date: December 2021

---