South Australian Protective Security Framework

Executive Guide

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

SOUTH AUSTRALIA

Government of South Australia

CONTENTS

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).

TERMINOLOGY

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

SAPSF EXECUTIVE GUIDE

PURPOSE

1. To provide each South Australian public sector agency[1] 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.

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 and Cabinet Circular 012 – Information Privacy Principles (IPPS) Instruction (PC012) states that the principal officer (accountable authority) must

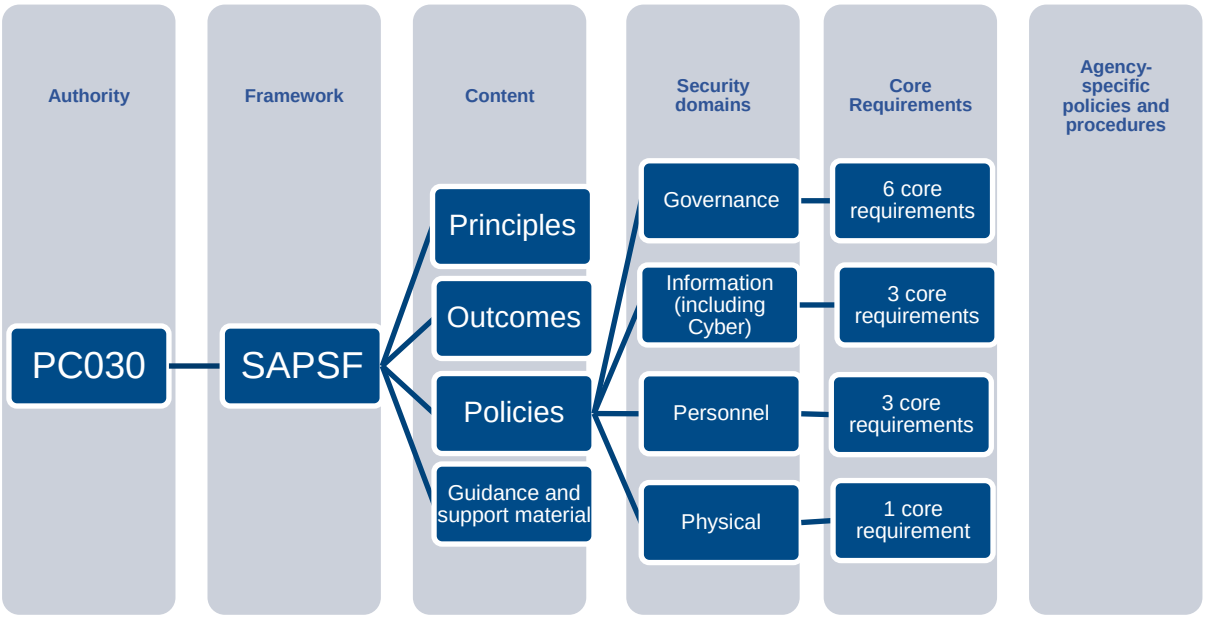
[1] See Applicability.

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.

PROTECTIVE SECURITY FRAMEWORK STRUCTURE

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



Principles

12. There are five (5) principles that form the foundation of the SAPSF. The cover the breadth of responsibilities under the SAPSF, and apply 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

13. 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.

14. 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

15. Information, people and assets are valuable resources to the South Australian Government.

16. Agencies have a responsibility to apply the right protections to their most valuable resources in line with the identified risk tolerance of the agency.

17. 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

18. 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.

19. 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

20. 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.

21. 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.

22. Accountability for the security of an agency's information, people and assets rests with the accountable authority[2], 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

23. 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.

24. The attitudes and behaviours of individuals contribute to building, but can also quickly erode, a strong organisational security culture.

25. 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.

[2] the person or group of persons responsible for, and with control over, the agency's operations

26. 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

27. 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

28. 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

29. 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

30. 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.

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/protective-security-framework/governance/govsec-1.

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[3] 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/protective-security-framework/governance/govsec-2.

[3] 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/protective-security-framework/governance/govsec-3.

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/protective-security-framework/governance/govsec-4.

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 mange 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/protective-security-framework/governance/govsec-5.

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[4]. 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/protective-security-framework/governance/govsec-6.

[4] 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[5]

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. apply the Minimum Recordkeeping Metadata Requirements Standard to ensure metadata reflects any protective markings

   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/protective-security-framework/information-security/infosec-1.

[5] 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[6] and meet any additional suitability requirements[7]

   IV. put in place an agreement or arrangement[8] 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/protective-security-framework/information-security/infosec-2.

[6] Some office holders are not required to hold a security clearance. See PSPF policy Access to Information for the full list.
[7] 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.
[8] 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/protective-security-framework/information-security/infosec-3.

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) Instructions

   II. undertake all mandatory pre-employment screening checks, including:

      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/protective-security-framework/personnel-security/persec-1.

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[9] 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/protective-security-framework/personnel-security/persec-2.

[9] Including eligibility waivers and conditional security clearance holders

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[10]

    c. employees transferring either temporarily or permanently to another state, territory or Commonwealth Government agency

    d. those taking extended leave[11].

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[12] 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[13]

    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/protective-security-framework/personnel-security/persec-3.

[10] 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.
[11] This policy does not define a period of time for where 'extended leave' applies. See Extended leave for more guidance.
[12] Including eligibility waivers and conditional security clearance holders
[13] Depending on the level of concern this **may** include the ASE, clearance sponsor, authorised vetting agency or the Australian Security Intelligence Organisation (ASIO)

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[14]

    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 https://www.security.sa.gov.au/protective-security-framework/physical-security/physec-1.

[14] ASIO Technical Notes are available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

DEFINITIONS

Term	Definition
accountable authority	the person or group of persons responsible for, and with control over, the agency's operations
accountable material	information which requires the strictest control over its access and movement
accreditation	the process of compiling and reviewing all applicable certifications and other deliverables to determine and accept the residual security risks
adversary	a party with interests counter to your own (e.g., foreign government, criminal element)
agency	as per the definition of public sector agency (as defined in section 3(1) of the *Public Sector Act 2009*) including administrative units, bodies corporate, statutory authorities and 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"
agency governance framework	the management structure used by an agency and the decision-making processes that define expectations, grant power or verify performance. (see also **governance**)
agency security committee	a management group that acts as the coordinator and adviser for all security aspects in relation to the scope of the agency's Cyber Security Program and/or Security Plan.
applicant(s)	the person or persons seeking employment with an agency
attestation	a declaration of attesting to the truth of something
authorised vetting agency	either the Australian Government Security Vetting Agency or another agency that has been authorised by AGSVA to undertake security vetting for its employees
availability	allowing authorised persons to access information for authorised purposes at the time they need to do so
biometrics	the technical term for body measurements and calculations – it refers to related human characteristics
bot	an automated piece of software designed to perform a certain task, often imitating or replacing a real person's user behaviour
business impact	the assessed impact upon business (individual, agency or government) operations from compromise of the information
caveat	a warning that the information contained has special protections *in addition to* those indicated by the classification
certification	establishing compliance with the minimum requirements of the certification authority; a certificate of conformance issued to an individual or organisation by an accredited body.
classification	an indication of the business importance and level of protection needed by information and assets to prevent compromise (for example **OFFICIAL: Sensitive**)
clearance sponsor	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 and South Australia Police (SAPOL) is an authorised vetting agency and clearance sponsor of SAPOL employees for NV1 and NV2 level security clearances
commencement	the point in time when a person begins in a new role or changes duties
compromise	includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure
confidentiality	limiting of access to information to authorised persons for approved purposes
consequence	the resulting effects that compromise of information could be expected to cause (commensurate with 'damage or business impact)

Term	Definition
container	physical container (such as a lockable cabinet or safe) used to store official information, most notably for sensitive and security classified information
contract	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 which outlines how the information is to be used and what protections **must** be applied (same as **service agreement**)
contractor	the external or third-party contracted to provide services to an agency (same as **service provider** and **supplier** and for the purposes of this policy, includes subcontractors)
critical process continuity plan	documented work-around plans for maintaining critical processes during a period of disruption at pre-determined acceptable levels
critical infrastructure	those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of South Australia as a State or affect South Australia's ability to support the conduct of national defence and ensure national security.
critical processes	agency processes that, if not performed, would eventuate in the highest level of risk to the agency. This could include meeting critical needs of the agency or satisfying mandatory regulations and requirements
critical service	services that, if compromised, would result in significant damage to the physical, social or economic wellbeing of the State. Critical Services are not typically ICT services, they are services that an agency delivers to the community on behalf of the State Government
cyber security	measures relating to the confidentiality, integrity and availability of information that is processed, stored and communicated by electronic or similar means. (synonymous with ICT Security)
cyber security program funding model	the combination of capital expenditure (CAPEX) during implementation of cyber security tasks and ongoing operational expenditure (OPEX) for ongoing maintenance and support.
damage	the resulting effects that compromise of information could be expected to cause (see **business impact**)
declassification	the process to reduce information to OFFICIAL (an unclassified state) when it no longer requires security classification access, handling and storage protections
eligibility	where the individual has the right to work in Australia, either as a citizen, or holding a valid work visa
encryption	a process, which may be irreversible, of transforming information, particularly data, into an unintelligible form
exemption	approval for exclusion from the implementation or use of a mandated document outlined in the SAPSF or SACSF
extreme vulnerability	a security vulnerability that could facilitate remote code execution or impact critical business systems, or an exploit exists in the public domain and is being actively used and/or the system is internet-connected with no mitigating controls in place
foreign actor	a person, group of people, company, agent or government of a country other than Australia
framework	a basic conceptual structure used to solve complex issues and/or address risks
function	the purpose or role an agency undertakes on behalf of the Government of South Australia
governance	system of decision-making, directing and controlling, through rules, relationships, policies, standards, systems and processes
guideline	additional, detailed advice on how to apply a policy.
handling	any processes for accessing, transmitting, transferring, storing or disposing of, official information

Term	Definition
harm	to cause injury or damage, either physically or psychologically, to another person or group of people
identity	who a person is, or the qualities or details that make them unique from others
incident	any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service and/or loss or corruption of information resulting in a breach or privacy or security
information assets	any information, or asset supporting the use of the information, that has value to the agency, such as collections of data, processes, ICT, people and physical documents
information custodian	the individual or group assigned responsibility for managing a set of information.
information owner	the individual or group responsible and accountable for a set of information. The information owner may, at their discretion, assign responsibility for management of the information to another person or group, also known as an information custodian.
insider threat	the risk posed to an agency from deliberate or accidental compromise to information and resources from employees or service providers (including contractors)
integrity	assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid
IT service recovery plan	a documented plan for restoring IT services following a disruption
likelihood	the chance of the risk event occurring
malicious insider	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
malware	malicious software
metadata	refers to a set of data about other data
misconduct	a breach of a disciplinary provision of the public sector code of conduct while in employment as a public sector employee, or other misconduct while in employment as a public sector employee
mobile device	mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices
multi-factor	a method of authentication using separate mutually dependent credentials, typically “something you have” and “something you know”
official information	all information created, sent and received as part of work of the South Australian Government
ongoing assessment	describes the processes and procedures for collecting and assessing information for the purposes of determining the suitability of an agency’s employees to maintain access to South Australian Government information and resources
originator	agency or individual that initially generated and/or is responsible for the information (also owner)
periodic	an event or action that must occur at prescribed intervals
personnel	all people that an agency employs (including contracted employees)
personnel security	the policies and procedures that seek to mitigate the risk of personnel exploiting access to an agency’s information or assets for unauthorised purposes
policy	a position or judgment with an across government focus, that describes actions or behaviours that must be followed
portable device	a small, lightweight device that is capable of storing and transferring large volumes of data (see also **mobile device**)

Term	Definition
position of trust	a position identified by the relevant agency that may require additional screening or other pre-employment measures according to the duties the role is required to perform; also any position or role within the agency with heightened levels of access to sensitive information or otherwise have increased risk profiles
procurement	the process of finding and agreeing to terms for the provision of goods and services
protection	the treatments, mitigations or controls implemented to prevent or minimise the likelihood, of compromise to an agency's people, information or assets
protective marking	identifies the level of classification and any other handling instructions or protections the information requires
ransomware	a type of malware designed to deny access to a computer system or data until a ransom is paid
reclassification	the administrative decision to change the security classification of information based on a reassessment of the potential impacts of its compromise
regular	an event or action that should occur at consistent intervals and may be determined by Standard Operating Procedures or a Security Schedule
resources	an agency's people, information and assets
risk appetite	the amount of risk an agency is willing to accept
risk-based approach	identifying and understanding the highest areas of risk and taking the appropriate mitigation measures in accordance with the level of risk
risk capacity	the maximum amount of risk (boundary) the agency can take and remain operational
risk profile	an outline of the risks to which an organisation, or business unit within an organisation, is exposed. Most Risk Profiles identify specific risks, associated mitigation strategies and an overall assessment or grading of each risk
risk tolerance	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
risk treatment	considered, coordinated and efficient actions and resources that mitigate or lessen the likelihood or negative consequences of a security risk
ruling	a specific application of security policy that must be adhered to by all agencies
screening	the processes associated with investigating the background of potential employees to determine their suitability to hold and undertaken the responsibilities of a position
security advisers	employees appointed within an agency to undertake specific responsibilities for security, such as Agency Security Advisors (ASA) and Information Technology Security Advisors (ITSA)
security assessor	reviews the system architecture, including security documentation, and assesses the implementation and effectiveness of security controls; typically an Information Security Registered Assessors Program (IRAP) assessor or entity personnel with the appropriate capability
security classified	indicates the information holds a classification of **PROTECTED, SECRET** or **TOP SECRET** and **must** be protected against compromise. Access to the information **must** be controlled and accessed by appropriately security cleared staff
security domains	the areas to which protective security requirements apply: governance, information, personnel, physical and cyber.
security maturity	a measure of an agency's security position within its risk environment and risk tolerances, while acknowledging progression toward security outcomes
security plan	how an agency articulates how its security risks have been identified, prioritised and will be managed in line with the agency's objectives
security risk	something that can result in compromise, loss, unavailability or damage to an agency's resources, including causing harm to people

Term	Definition
security zone	a scalable physical security measure to protect the resources or assets within an agency's facilities
senior leadership	generic term that may encompass the Agency Board, Senior Executive Members, Chief Executive, Agency Security Executive or equivalent
sensitive	indicates information requires *some* level of protection but is not security classified
separation	the process where employees permanently or temporarily leave their employment with an agency
shared risk	security risks that emerge from a single source and extend across multiple agencies and/or their premises, that impact the community, industry and international or interstate jurisdictions or partners
social engineering	deceiving or manipulating people into divulging confidential or personal information that may be used for fraudulent purposes
spam	an unsolicited or undesired electronic message
stakeholder	a person, group or agency with an interest in the security of an individual or entity
standard	a formal document that provides a set of rules to support compliance with a policy
strategy	a plan of action, or direction, designed to achieve a particular goal
subcontractor	a person or entity that undertakes work or duties on behalf of a **contractor**
suitability	the combination of eligibility and fit for the role, assessment of integrity and ability to meet the assessment criteria or other requirements
supplier	any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency (see also **contractor**)
supplier access	any local or remote access made by a supplier to Government IT assets, as defined in contracts and/or service level agreements
threat	a declared intent to inflict harm on personnel or property
user	anything that accesses ICT resources, including persons and computer systems
value	the assessed importance of the information based upon the potential consequences of compromise – (including but not limited to, monetary value)
visitor	any person who is not an agency employee with ongoing access to agency facilities
vulnerability	the degree of susceptibility and resilience of an agency to risks and threats
zone	the physical entities and workspaces in which official information is produce, accessed, handled and stored (see also **security zone** and **zoning**)
zoning	the process for determining the appropriate security zone and implementing required control elements

Acronyms

Acronym	Words
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGSVA	Australian Government Security Vetting Agency
ASA	Agency Security Adviser
ASD	Australian Signals Directorate
ASE	Agency Security Executive

Acronym	Words
ASIO	Australian Security Intelligence Organisations
ASIO-T4	ASIO Protective Security capability
BIL	Business Impact Level
CCTV	Closed Circuit Television
CI-HR	Critical Infrastructure High-Risk
DHS	Department of Human Services
DLM	Dissemination limiting marker
DPC	Department of the Premier and Cabinet
DTF	Department of Treasury and Finance
DVS	Document Verification Service
EACS	Electronic Access Control System
ICS	South Australian Information Classification System
ICT	Information and Communication Technology
IMM	Information Management Marker
IPPS	Department of the Premier and Cabinet Circular PC012 – Information Privacy Principles Instruction
IRAP	Information Security Registered Assessors Program
ISM	Australian Government Information Security Manual
ISMF	Information Security Management Framework
ITSA	Information Technology Security Adviser
LSA	Lead Security Agency
MFA	Multi-factor Authentication
NTK	Need-to-know principle
PC012	Premier and Cabinet Circular 012 – Information Privacy Principles 012 (see IPPS)
PC030	Primer and Cabinet Circular 030 – Protective Security in the Government of South Australia
PC042	Premier and Cabinet Circular 042 – Cyber Security Incident Management
PIDS	Perimeter Intrusion Detection System
PSO	Protective Security Officer
PSPF	Protective Security Policy Framework (Commonwealth)
PSSB	Police Security Services Branch
SACSF	South Australian Cyber Security Framework
SAES	South Australian Executive Service
SAPOL	South Australia Police
SAPSF	South Australian Protective Security Framework
SAS	Security Alarm System
SCC	State Crisis Centre (South Australia)
SCEC	Security Construction and Equipment Committee (Commonwealth)

Acronym	Words
SCIF	Sensitive Compartmented Information Facility
SEC	State Emergency Centre (South Australia)
SEEPL	Security Equipment Evaluated Product List
SMSMP	Sensitive Material Security Management Protocol
TCSM	Technical Counter Surveillance measures
VEVO	Visa Entitlement Verification Online

RELATED DOCUMENTS

- South Australian Protective Security Framework
- South Australian Cyber Security Framework (SACSF)
- Protective Security Act 2007
- 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: Chief Executive, Department of the Premier and Cabinet	Date of first approval: 20 April 2020
Revision number: 2.0	Date of review: 30 November 2022
Next review date: December 2024	Contact: sapsf@sa.gov.au

For more information:

National and Protective Security
Security, Emergency & Recovery Management
Social Policy and Intergovernmental Relations
Department of the Premier and Cabinet

E SAPSF@sa.gov.au
W security.sa.gov.au

SOUTH AUSTRALIA

Government of South Australia