South Australian Protective Security Framework

# GOVSEC 4

## ANNUAL SECURITY ATTESTATION

SOUTH AUSTRALIA

Government of South Australia

# CONTENTS

# POLICY

## PURPOSE

1. The policies of the South Australian Protective Security Framework (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

**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[1] **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

[1] This policy 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".

# GUIDANCE

## ANNUAL SECURITY ATTESTATION

4. The annual attestation is a summary of an agency's protective security performance over the previous 12-month period in relation to the security outcomes and core requirements of the SAPSF, as established in the agency's security plan.
5. The accountable authority of each agency **must** complete and submit the annual security attestation to the Department of the Premier and Cabinet (DPC) to demonstrate the degree to which the agency has implemented the necessary protective security measures to protect its people, information and assets, consistent with the objectives of the agency's security plan and the requirements of the SAPSF.
6. The annual security attestation **must** be submitted by agencies by 30 June of each calendar year taking into account the protective security performance of the preceding 12 months. Submissions are to be sent to sapsf@sa.gov.au.

## IDENTIFYING PROGRESS AGAINST SECURITY GOALS AND STRATEGIC OBJECTIVES

7. This element presents as an 'executive summary' of an agency's security program over the preceding 12 months. The content of this element **should** align to the security goals and strategic objectives of the security plan.
8. Agencies are encouraged to include any highlights from the previous 12 months, for example, milestones or achievements that have been made in developing the security culture or maturity of the agency.

## DEPARTURE FROM SAPSF CORE OR SUPPORTING REQUIREMENTS

9. As per SAPSF policy **Security governance**[2], the accountable authority of an agency **must** put in place protective security arrangements that implement the core and supporting requirements of the SAPSF, unless relevant circumstances prevent an agency from doing so.
10. Agencies **must**, in their annual security attestation:

    I. detail the circumstances preventing the implementation of the core or supporting requirement(s)

    II. outline the alternative arrangements being implemented, including any justifications based upon the agency's security maturity and risk tolerance

    III. outline actions planned to move toward achieving the requirements of the SAPSF and/or further reducing risk

## CHALLENGES AND BARRIERS

11. Agencies **should** highlight any challenges or barriers that were encountered to achieving the agency's security plan or the requirements of the SAPSF. Sharing challenges and barriers to effective protective security can serve as a useful source of information for broader improvements to the SAPSF and enable useful solutions or risk treatments to be identified from across government.

[2] See Implementing core and supporting requirements of the SAPSF in SAPSF policy Security governance for more detail.

12. Challenges or barriers **may** include:
    - financial
    - resources
    - capability
    - legislative restrictions
    - external third-party dependencies
    - machinery of government
    - difficulty assigning appropriate security responsibilities
    - low security awareness/understanding of core/supporting requirements
    - other
13. Where challenges or barriers are identified, agencies **should** indicate how they plan to address any shortfall in protective security effectiveness, or strategies to overcome those challenges or barriers in future.

## SECURITY MATURITY

14. Security maturity is a meaningful way to demonstrate progress to achieving or exceeding the minimum standards of the SAPSF while factoring in the specific risk environment and risk tolerance of individual agencies.
15. Security maturity considers how holistically and effectively each agency:
    IV. understands, prioritises and manages its security risks
    V. responds to and learns from security incidents
    VI. fosters a positive security culture
    VII. achieves security outcomes and core requirements while delivering business outcomes.
16. To create consistency across the South Australian Government, SAPSF policy Security planning **recommends** agencies establish maturity targets within their security plan. **Table 1** contains the four levels of security maturity levels of the SAPSF.

**Table 1 – Security maturity levels**

| Maturity level | Definition | Target |
|---|---|---|
| **1 Informal** | Security is ad-hoc, unmanaged and unpredictable. Security success relies on individuals rather than effective processes. | Not recommended as a maturity target as it reflects a lack of capability maturity |
| **2 Basic** | Policies and processes are in place to meet the core and supporting requirements of the SAPSF, but security management is mainly reactive and inconsistent. | This level is reflective of developing capability maturity and may be appropriate as a stepping-stone to a higher maturity target |

| Maturity level | Definition | Target |
|---|---|---|
| **3 Managed** | Security of the agency is risk-based, fit-for-purpose measure are in place, understood and consistently followed. Ongoing investment is required to sustain measures at this level. | Managed is considered the effective implementation of the SAPSF core and supporting requirements. |
| **4 Enhanced** | Security capability is adaptable to a dynamic, high-risk operating environment. Security culture is embedded and security goals and objectives are consistently exceeded. | Target should be selected if risks identified require enhanced security measures. |

17. Agencies **should** consider the security maturity indicators (see Annex A of Security planning) when setting maturity targets and assessing security maturity.
18. Agencies **must** assess their progress to achieving their maturity target, include any evidence to support that assessment and what further steps are to be taken to either meet, or enhance, the maturity level achieved in the following 12 months.

## SAPSF SECURITY ROADMAP

19. It is **recommended** agencies use the **SAPSF Security Roadmap** when assessing their security maturity. The roadmap enables agencies to consolidate all the relevant information into a single document that can then be used as the basis for completing the annual security attestation.

# IDENTIFYING SECURITY RISKS

21. Identifying the security risks affecting an agency provides valuable insights for agency and government decision-makers into risks that are:

    I. systematic or emerging

    II. not sufficiently mitigated

    III. insufficiently covered by protective security policies

22. Evidence collected from agencies and analysed directly helps to inform strategies to mitigate security threats and vulnerabilities across government.

23. Agencies **must** provide details of their key security risks across each of the four security domains (including ICT), and the risk treatments being used.

## NEW AND EMERGING RISKS

23. The security risks on an agency may be influenced or changed by factors such as the risk environment, operational priorities and security incidents. The priority of risks across an agency may change year by year as a result. SAPSF policies Security planning and Security monitoring provide guidance to assist agencies in identifying, prioritising and monitoring their security risks to ensure protective security risk treatments are appropriate and effective.

24. Security plans themselves **should** be treated as dynamic documents which react and respond to changes in the risk environment or objectives of the agency. As such,

agencies **must** be vigilant in identifying new or emerging risks that would require amendment to the security plan to mitigate against uncontrolled risks to people, information and assets.

## RISKS TO OTHER AGENCIES OR PARTIES

25. SAPSF policy Security planning (see paragraph 43. Shared risks) requires agencies to identify risks that might impact on, or be influenced by, other agencies or parties, and to ensure a high level of cooperation and communication between agency stakeholders to mitigate those risks.
26. Where an agency identifies a new risk, or a risk that was previously unknown, which impacts upon another agency or party, details of this risk **must** be shared with the affected agencies or parties to ensure controls can be implemented and the risk mitigated as best as possible.
27. If an agency identifies a short-fall in its own security maturity relating to a core or supporting requirement of the SAPSF, the result of which increases the risk to another agency or stakeholder, the agency **must** notify the affected agencies of the increased security risk, as well as any proposed controls to mitigate the risk.

## REPORTING ON SIGNIFICANT SECURITY INCIDENTS

28. A significant security incident is a deliberate, negligent or reckless action that leads, or could lead, to compromise of official information or resources. Agencies are required to report significant security incidents to the SAPSF team in addition to all relevant authorities, or affected agencies. Any significant security incidents should be included in the annual security attestation. SAPSF policy Security Governance contains more detail surrounding the reporting of security risks.

# 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: 26 October 2022 |
| Next review date: December 2024 | Contact: sapsf@sa.gov.au |

# CHANGE LOG

| Version | Date | Changes |
|---|---|---|
| 1.0 | 20/04/2020 | First issue of policy |
| 2.0 | 26/10/2022 | Policy reviewed, no change |



Government
of South Australia