South Australian Protective Security Framework

# GOVSEC 1

## SECURITY GOVERNANCE

SOUTH AUSTRALIA

Government of South Australia

# CONTENTS

# POLICY

## PURPOSE

1. This policy describes how an agency's accountable authority[1] 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

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

## SUPPORTING REQUIREMENTS

2. To ensure an agency[2] 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:

      b. appointing security advisers (ASAs and 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.

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

[2] 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

## ROLE OF THE ACCOUNTABLE AUTHORITY

3. The accountable authority for each agency is responsible to their portfolio minister and the South Australian Government for their agency's people, information and assets.

4. In establishing the protective security arrangements for an agency, the accountable authority must ensure:

   I. business continuity during security incidents, disruptions or emergencies

   II. the safety of employees to carry out the functions of government and those dealing with the agency (including visitors)

   III. the protection information and resources held within the agency.

## RESPONSIBILITIES OF THE ACCOUNTABLE AUTHORITY

5. The accountable authority of the agency must:

   I. implement the SAPSF core and supporting requirements

   II. appoint an Agency Security Executive (ASE) to be responsible for directing protective security and authorised to make security decisions, including the appointment of ASAs and ITSAs [3]

   III. ensure they have employees who hold the appropriate level of clearance to access security classified information, including themselves, where there is a need to share highly sensitive, or even security classified information of relevance to security with other agencies or entities

   IV. ensure security awareness training is provided for all employees and service providers (including contractors) outlining their security responsibilities, including how to manage security risks

   V. embed effective security risk management processes

   VI. approve the agency's security plan for managing security risks

   VII. ensure the security of the agency's ICT systems is consistent with the requirements of SAPSF policy Robust ICT and cyber security and the South Australian Cyber Security Framework (SACSF)

   VIII. promote and foster a positive security culture with defined expectations and priorities

   IX. monitor the agency's security maturity

   X. assess the agency's security maturity in the annual security attestation

   XI. approve citizenship and uncheckable background waivers for security clearance applications.[4]

## IMPLEMENTING CORE AND SUPPORTING REQUIREMENTS OF THE SAPSF

6. The accountable authority is responsible for putting in place protective security arrangements that implement the core and supporting requirements of the SAPSF, unless relevant circumstances prevent an agency from doing so.

[3] For smaller agencies, the accountable authority **may** decide to appoint themselves as ASE, and delegate the day-to-day functions of protective security to appointed security advisers.

[4] For more information, see SAPSF policy Recruiting employees.

7. Relevant circumstances may include:
   - circumstances outside of the agency's control
   - where the cost or impact of implementing the requirement would prohibit the agency's ability to perform its core function
   - where alternate arrangements are implemented that achieve the same or greater security outcomes that the core or supporting requirement
8. In such circumstances, the accountable authority of the agency must:
   - I. identify and document 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
   - IV. include a record of all decision-making in the agency's annual security attestation.
9. Under section 12 of the Public Sector Act 2009, the accountable authority of all agencies must notify their responsible minister(s) of all significant issues affecting the agency. Any significant issues[5] affecting the agency in respect of implementation or application of the SAPSF must be included.
10. Deliberately disregarding implementing the SAPSF or its requirements is considered a security incident. For information on managing security incidents see SAPSF policy Annual security attestation.

## SECURITY CLEARANCES FOR AGENCY SECURITY PERSONNEL

11. From time to time, there may be a need to share highly sensitive, or even security classified information with other agencies or entities. In such cases, the accountable authority is responsible for ensuring they have employees who hold the appropriate level of clearance to access security classified information, including themselves.
12. It is strongly recommended that the accountable authority of each agency obtain a security clearance to at least the level of Negative Vetting Level 1 (NV1). Any employees who are also connected in a workflow involving security classified information (including handling of documents, system administration, access privileges etc.) must also obtain a security clearance to the same level as the accountable authority.
13. It is also strongly recommended that all agency security personnel (ASE, ASA, ITSA etc.) also obtain security clearances to a level deemed appropriate by the accountable authority.
14. Information on obtaining security clearances can be found in SAPSF policy Recruiting employees.

## LEAD SECURITY AGENCIES

15. Some agencies have additional protective security responsibilities under this policy. An agency will be designated a Lead Security Agency (LSA) where it is a:
    - I. provider of government protective security policy or advice

[5] It is not considered a reportable significant issue if the alternative mitigations put in place provide the same (or exceed the level of) protection as the SAPSF requirement.

II. provider of shared-services arrangements.

16. Table 1 lists the LSAs for the South Australian Government.

**Table 1 - Lead Security Agencies in South Australia**

| Agency | Protective Security Responsibility |
|---|---|
| **Department of the Premier and Cabinet (DPC)** | • Lead policy agency for the SAPSF and SACSF<br>• State government AGSVA security clearance sponsor<br>• Provider of central government ICT services<br>• Lead agency for cyber security, including major incident coordination and Cyber Watch Desk |
| **South Australia Police (SAPOL)** | • Responsible for the protection of designated Critical Infrastructure-High Risk (CI-HR) assets across South Australia as required by the *Protective Security Act 2007* through the **Protective Security Services Branch (PSSB)**<br>• Authorised vetting agency for SAPOL clearances (NV1 & NV2 level) |
| **State Records of South Australia** | • Responsible for South Australian records, information standards and advice |
| **Department of Human Services (DHS)** | **Screening Unit:** provision of worker and volunteer related checks<br>• child-related employment and working with children checks<br>• disability services employment<br>• aged-care sector employment |

## PROVIDING ADVICE AND SUPPORT

17. A LSA provides other South Australian Government agencies with advice and/or services relating to government security. Timely and considered security support and advice is critical to ensuring the maintenance of protective security requirements across the public sector.

18. LSAs are required to provide advice and support which helps other agencies achieve and maintain an acceptable level of security, appropriate to their risks, in line with government-wide security policies, priorities and plans.

19. It is recommended that LSAs:

I. implement appropriate oversight arrangements to coordinate security services provided to other agencies

II. maintain the capability to provide timely and accurate security advice and services

III. maintain regular contact with supported agencies to increase awareness and effectiveness of the LSAs role and capabilities

IV. schedule periodic review of the service arrangements and make procedural adjustments where necessary.

20. The accountable authority of an LSA must establish and agree upon clearly defined accountabilities, responsibilities and procedures for entering into partnerships or service provision arrangements with other agencies.

## SUPPORTED AGENCIES

21. Supported agencies are those that receive direct support or services from a LSA. It is recommended that the accountable authorities of both the LSA and the supported

agency establish a formal agreement or arrangement that outlines the provision of services and the proscribed responsibilities of each party.

22. It is recommended that supported agencies notify any relevant LSAs of significant changes to protective security arrangements or agency risk profile.

23. Supported agencies should seek clarification if arrangements between the LSA and supported agency are unclear regarding agreed responsibilities during a significant or reoccurring security incident or event. This may include:

    I. who takes control and when

    II. who has authority under what circumstances

    III. to whom and when an incident is escalated

    IV. communication lead during a significant or reoccurring incident or event.

24. The accountable authority of a supported agency remains responsible for the overall security of their agency. The accountable authority of a supported agency may outsource responsibility for specific security functions under shared-services or a partnership agreement, however, they should seek agreement from the accountable authority of a LSA.

## SECURITY RISK MANAGEMENT

25. Overall security risk management responsibility rests with the accountable authority. This means the accountable authority must:

    I. determine the agency’s tolerance for security risks

    II. apply a risk-based approach to manage the agency’s security risks

    III. consider any implications risk management decisions have on the security or operations of other agencies and share information where appropriate.

26. Determining agency risks mean identifying, assessing and prioritising risks to people, information and assets and should result in the effective risk-based application of mitigations or protections that minimise, monitor and control the likelihood and consequences of risks.

27. Further information about security risk management and security planning can be found in the SAPSF policy Security planning.

## AGENCY SECURITY EXECUTIVE

28. The accountable authority must appoint a South Australian Executive Service (SAES) (or equivalent) ASE to be responsible for directing all areas of security in the agency. The appointed ASE should be at a level appropriate to managing critical, security-related risks, incidents or emergencies within the agency.

29. The ASE should have sufficiently experience or training to perform the required security functions. The ASE must have a direct report to the accountable authority.

30. The ASE supports the accountable authority by providing strategic oversight of protective security to assist the continuous delivery of business operations, and by fostering a positive security culture through the application of policies and practices that embed security into agency operations.

31. The ASE must be empowered and resourced to make security related decisions including:

    I. appointing security advisers (ASAs and ITSAs) within the agency

    II. agency protective security planning

    III. agency protective security practices and procedures

IV. investigating, responding to, and reporting on security incidents.

## RESPONSIBILITIES OF THE ASE

32. The ASE of the agency must:

I. support the accountable authority to ensure the safety of all people (including contractors, visitors and clients), information and assets

II. report directly to the accountable authority on security, including security incidents or matters

III. appoint sufficient security personnel (including but not limited to ASAs and ITSAs) to perform the security functions of the agency and oversee performance of their security responsibilities (see Appointing security advisers).

IV. set the strategic direction for protective security planning and risk management (see SAPSF policy Security planning)

V. embed security procedures that achieve the security outcomes of the SAPSF, consistent with all legislative and other policy requirements

VI. manage the agency's response to security-related incidents or matters in accordance with agency security procedures

VII. embed security monitoring mechanisms across the agency to support investigating, responding and reporting on security incidents

VIII. foster a positive security culture where employees are aware of and understand their security responsibilities and are empowered to manage security risks

IX. establish security performance measures to help determine effectiveness of security arrangements, identify new risks, counter risks above the agency's tolerance and improved security maturity (see SAPSF policy Security monitoring)

X. managing and disseminating security related information across the agency, including sharing threat-related information with staff when required

XI. oversee preparation of the agency's SAPSF annual security attestation for approval by the accountable authority.

## SECURITY GOVERNANCE COMMITTEE

33. It is recommended that the ASE establish and oversee (as chair) a security governance committee comprising relevant security personnel from within the agency. [6]

34. A security governance committee provides support to the accountable authority and ASE by:

- providing a cohesive and coordinated approach to risk and security
- fostering a positive security culture
- contributing to longer-term agency security planning
- monitoring existing security plans and identifying and managing risks
- considering and reviewing the outcomes of security incidents and investigations
- facilitating information sharing for security improvements.

[6] The ASE **may** determine that a security oversight committee is **not required** in line with the size and function of the agency.

## APPOINTING SECURITY ADVISERS

35. The ASE is responsible for appointing security advisers (ASA and ITSA) for the agency. The ASE must appoint enough security advisers to account for the security requirements of the agency across the four protective security domains: governance, information (including ICT), personnel and physical. There is no maximum number of security advisers that can be appointed.

36. In making these decisions, the ASE must:

    I. consider the scope and responsibilities delegated to each position within the context of the agency's risk environment and tolerance, size and function

    II. consider the appropriate arrangements for managing the responsibilities of all security advisers[7]

    III. consider appointing security advisers at a level that requires only broad direction in terms of delivering objectives or the requirements of the SAPSF

    IV. ensure delegations allow security advisers to undertake specific actions in line with the policies of the agency, or to review previous actions or decisions taken of relevance to security

    V. consider the appropriate competencies, experience, specialist skills or qualifications required to undertake the protective security requirements of the agency.

## AGENCY SECURITY ADVISERS

37. The ASE must appoint at least one ASA for the agency. An ASE may determine it is appropriate to appoint additional ASAs to functions, depending on the size and function of the agency. It is recommended any additional advisers are designated 'Deputy ASA'.

38. An ASE may determine it is appropriate to delegate security functions to an ASA across multiple security domains, or to appoint multiple ASAs to functions within the same domain.

39. If the agency performs a diverse function or has responsibilities across a diverse range of locations or operational environments, it may be more appropriate for the ASE to appoint security advisers at each location.[7]

40. The suggested security functions of ASAs are listed in Table 2 according to the four security domains.

**Table 2 – Suggested functions of ASAs**

| Domain | Suggested Security Adviser Functions |
|---|---|
| **Governance** | Assist the ASE by:<br>• demonstrating a sound knowledge, and ability to apply, the requirements of the SAPSF<br>• providing advice on protective security and security risk management arrangements<br>• identifying and supporting management of governance security risks |

[7] If an agency's arrangements result in the security adviser **not** reporting directly to the ASE, the ASE **must** maintain visibility of performance and outcomes of security responsibilities.

| Domain | Suggested Security Adviser Functions |
|---|---|
|  | • ensuring security plans and procedures are effective in achieving specified security outcomes<br>• monitoring security systems that facilitate the agency's capacity to function and identify security risks<br>• preparing security reports for the ASE or security committees, and assisting with gathering information to meet annual security attestation obligations<br>• coordinating and conducting security reviews<br>• liaising with law enforcement and intelligence agencies, other emergency services, service providers, clients and stakeholders<br>• responding to and coordinating security incident arrangements and being accessible for employees to discuss security issues or concerns<br>• managing simple security investigations and escalating complex investigations to the ASE<br>• promoting the security and risk culture where personnel value and protect government information and assets<br>• establishing networks and relationships to understand the agency's business functions and vulnerabilities<br>• ensuring security requirements are considered in other agency plans such as business continuity, fraud control and awareness. |
| **Information** | Assist the ASE by:<br>• demonstrating a sound knowledge, and ability to apply, the requirements of the SAPSF<br>• identifying and managing information risks<br>• ensuring appropriate procedures are established (in accordance with the SAPSF) for the handling and protective marking of information<br>• managing access to information<br>• in consultation with the agency's ITSA, ensure ICT systems are protected against unauthorised access or compromise and information in electronic form is stored, processed, and communicated in accordance with the law, South Australian Government policies[8], and the information security requirements detailed in the agency's security plan<br>• providing briefings and advice to agency employees on information and ICT security, including briefings to employees located or travelling overseas |
| **Personnel** | Assist the ASE by:<br>• demonstrating a sound knowledge, and ability to apply, the requirements of the SAPSF<br>• identifying and managing personnel security risks<br>• managing the agency's personnel security program<br>• developing and conducting security awareness training programs (including refresher and specialised training)<br>• managing eligibility and suitability of personnel procedures<br>• monitoring ongoing assessment of personnel<br>• coordinating the personnel security aftercare program for separation of employees, including withdrawing accesses and informing about ongoing security obligations |

[8] Such as the *Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions,* on access to, disclosure or use of, personal information collected or received

| Domain | Suggested Security Adviser Functions |
|---|---|
| | • providing advice on personnel security, including briefings to employees located or travelling overseas. |
| **Physical** | Assist the ASE by:<br>• demonstrating a sound knowledge, and ability to apply, the requirements of the SAPSF<br>• identifying and managing physical security risks<br>• ensuring a safe and secure physical environment for all personnel that come into contact with the agency<br>• ensuring a secure physical environment for official resources<br>• managing physical security measures and access controls to protect facilities, information and physical assets, for example certification of security zones<br>• liaising with and managing security contractors in the delivery of security services, including:<br>○ Security Construction and Equipment Committee (SCEC) endorsed consultants<br>○ security industry specialists<br>○ security guards (guarding)<br>○ safe hand and overnight couriers<br>○ secure destruction<br>○ locksmithing services.<br>• undertaking strategic planning for preparation of new or green-field sites |

## INFORMATION TECHNOLOGY SECURITY ADVISERS

41. The ASE must appoint at least one ITSA for the agency. An ASE may determine it is appropriate to appoint additional ITSAs to functions, depending on the size and function of the agency. It is recommended any additional advisers are designated ‘Deputy ITSA’.

42. If the agency performs a diverse function or has responsibilities across a diverse range of locations or operational environments, it may be appropriate for the ASE to appoint ITSAs at each location.[7]

43. Some suggested security functions of ITSAs are listed in Table 3. Guideline 5 of the SACSF provides additional guidance on the roles and responsibilities of ITSAs.

**Table 3 - Suggested functions of ITSAs**

| Domain | Suggested Security Adviser Functions |
|---|---|
| **Information (ICT)** | Assist the ASE by:<br>• understanding and implementing the requirements of the SACSF in line with the agency’s risk assessment and operational requirements<br>• identifying and managing information and ICT security risks<br>• providing advice on protective security and security risk management arrangements |

| | |
|---|---|
| | • ensuring appropriate procedures are established (in accordance with the SAPSF and SACSF for the handling and protective marking of information<br>• ensuring the agency's ICT systems are protected against unauthorised access or compromise, and information in electronic form is stored, processed and communicated in accordance with the law, South Australian Government policies[9] and the information security requirements detailed in the agency's security plan<br>• safeguarding information from cyber threats, ensuring robust ICT systems contributing to personnel awareness of information security obligations around appropriate use of ICT equipment and official information<br>• responding to and managing information or ICT security incidents and ensuring they are reported to the Office for Cyber Security as per the across government incident reporting scheme.<br>• providing briefings and advice to agency employees on information and ICT security, including briefings to employees located or travelling overseas<br>• preparing security reports for the ASE or security committees, and assisting with gathering information to meet annual security attestation obligations<br>• coordinating and conducting ICT security reviews<br>• promoting the security and risk culture where personnel value and protect government information and assets<br>• liaising with law enforcement and intelligence agencies, other emergency services, service providers, clients and stakeholders<br>• liaising with and managing ICT contractors in the delivery of secure services including:<br>○ telephones<br>○ internet and email gateways<br>○ data storage and recovery |

## PROTECTIVE SECURITY PLANNING, PRACTICES AND PROCEDURES

44. All agencies are required to have a security plan which establishes the strategic direction and sets the expectations for efficient and effective security management practices for the agency (for more information see SAPSF policy Security planning).

45. The ASE is responsible for establishing the strategic direction, allocating resources in line with the strategy and improving the security maturity of the agency.

[9] Such as the SACSF and Premier’s Circular PC012 Information Privacy Principles (IPPS) Instructions (PDF, 643.3 KB)

46. Planning must incorporate developing practices and procedures that identify, manage and mitigate security risks and which enable the agency to continue to deliver effective and efficient government services.

47. Effective practices and procedures are those that are embedded into day-to-day operations, are well understood by all employees and demonstrated by senior management. Effective practices and procedures are also those which assist to identify changes to the risk environment and can be updated accordingly.

48. Security practices and procedures must be designed to deliver the agency's security plan which can in turn be useful in determining the agency's security maturity and overall implementation of the SAPSF.

## MANAGING SECURITY INCIDENTS

49. Effective management of security incidents reduces the consequences from threats, behaviours or events while reducing the likelihood that they will re-occur.

50. Agencies must implement practices and procedures to detect, respond, investigate and report security incidents. Furthermore, information gathered following a security incident will help to determine the effectiveness of existing agency protective security arrangements, assess agency security maturity and culture, and highlight any vulnerabilities.

51. A security incident is defined as:

    I. an action, whether deliberate, reckless, negligent or accidental that fails to meet protective security requirements or agency practices and procedures that results, or may result, in compromise to official information or resources

    II. an approach, from anybody seeking unauthorised access to official information or resources

    III. an observable occurrence or event[10] that can harm South Australian Government people, information or assets.

52. A significant security incident is a deliberate, negligent or reckless action that leads, or could lead, to compromise of official information or resources. Table 4 provides some examples of significant security incidents.

**Table 4 – Security incidents**

| Examples of security incidents | Examples of significant security incidents |
|---|---|
| Criminal actions such as actual or attempted theft, break and enter, vandalism or assault | Espionage or suspected espionage |
| Loss of personal information that is likely to result in serious harm | Actual or suspected compromise of material at any level, including tampering with security containers or systems |
| Security classified material not properly secured or stored | Loss, compromise, suspected compromise, theft or attempted theft of classified equipment |
| Security classified material left in inappropriate waste bins or government assets to be sold or disposed of | Actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored |

[10] E.g. natural disaster, terrorist attacks etc.

| Examples of security incidents | Examples of significant security incidents |
|---|---|
| Deliberate disregard of implementing an SAPSF requirement | Loss of material classified PROTECTED or above, or significant quantities of material of a lower classification |
| Access passes or identification documents lost or left unsecured | Recovery or previously unreported missing classified material or equipment |
| Incorrect handling of security or classified marked information, such as a failure to provide the required protection during transfers or transmission resulting in a data spill on an electronic information network or system | Unauthorised disclosure of official or classified information, significant loss or compromise of cryptographic keying material, or a significant breach of ICT systems. |
| Compromise of keys to security locks, or of combinations settings | Continuous breaches involving the same person or work area where the combination of the events warrants an investigation |
| Sharing computer passwords | Loss, theft, attempted theft, recovery or suspicious incidents involving weapons, ammunitions, explosives or hazardous materials including chemical, biological, radioactive or nuclear. |
| Vandalism | Actual or suspected hacking into any ICT system |

## DETECTING SECURITY INCIDENTS

53. Early detection of a security incident and timely response is critical to reducing the consequences from that incident. Establishing mechanisms to enable possible or actual security incidents to be communicated to agency security management in a timely manner is essential to effective security risk management.
54. Agencies must ensure that all employees understand when and how to report potential incidents or concerns. It is recommended that security incident reporting be included in agency security awareness training.
55. While reporting is a common means of detecting security incidents, it is recommended that ASEs consider other security monitoring measures to assist in identifying potential or actual security incidents.

## RESPONDING TO SECURITY INCIDENTS

56. All agencies must establish procedures for managing security incidents. Incident management procedures should be consistent, appropriate and fair and be applicable to any security incident that may arise.
57. Table 5 provides some recommended elements to consider in developing incident management procedures.

**Table 5 – Recommended incident management procedures**

| Procedure |
|---|
| • Employees and service providers (contractors) should report security incidents to a centralised point in the agency (e.g., ASE or security advisers). Arrangements for employees travelling or working remotely should be considered |

- Formal procedures and mechanisms to make it easy to report security incidents (including for responding to incidents that occur outside of an agency's premises) should be considered

- ASEs, ASAs and ITSAs should maintain records of reported incidents and other security incidents

Handling procedures once a security incident has been reported, should include:

- clearly defined roles and responsibilities of security personnel involved in managing the security incident
- clearly defined escalation points, chains of command, communication channels (both internal and external)
- timeframes for incident response and recovery
- assessment and categorisation of the level of ham or compromise
- any technical requirements or business resumptions arrangements
- prioritisation mechanism for multiple or simultaneous incidents
- agency-specific incidents or types of incidents
- linkages to other agencies' procedures, such as business continuity plans or disaster recovery plans
- incident reporting to the accountable authority, ASE, and/or security governance committee
- testing and review cycles

- Feedback processes should be included to ensure all relevant parties are notified of results once and incident has been resolved.

- recording security incidents to create a valuable source of data to assess an agency's security environment and performance. The ASE should maintain oversight of security records and regularly analyse to identify trends or systematic issues.

## INVESTIGATING SECURITY INCIDENTS

58. ASEs must determine when a security incident is significant enough to warrant an investigation. Security incidents can be actual or suspected, and an investigation may be required to resolve an existing breach or vulnerability and reduce the impact or consequences. Investigations may also provide useful information for future risk assessments or reviews and will help to validate existing protective security arrangements within the agency.

59. A security investigation:

    I. is a formal process examining the cause and extent of the security incident that has, or could have, caused harm to individuals, or another agency or the state or national interest

    II. gathers evidence that may be admissible for any subsequent action (criminal, civil penalty, civil, disciplinary or administrative sanctions)

    III. prevents re-occurrence of the incident by implementing improvements to the agency's systems or procedures

    IV. protects the interest of the South Australian Government and the rights of the affected individuals.

60. The ASE is responsible for ensuring the agency has procedures in place to conduct security investigations, when required. It is recommended that those procedures cover:

    I. terms of reference and the investigation plan (authorised by the accountable authority or ASE)

    II. responsibilities of the investigator, approving officer and other relevant parties

III. qualifications and/or training required for investigators

IV. procedural fairness and standards of ethical behaviour to ensure impartiality and the absence of any conflicts-of-interest

V. actions for handling complaints or allegations (including anonymous or public interest disclosure reports)[11]

VI. case management procedures to ensure compliance with the agency's procedures

VII. procedures for undertaking operational practices (such as interviews of affected persons)

VIII. points of referral, escalation or approval, including keeping the ASE notified of progress

IX. points of escalation to law enforcement or the Australian Security Intelligence Organisation (ASIO)

X. findings and recommendations

XI. final report requirements.

61. The ASE is responsible for assessing the requirement for a formal security investigation. In assessing the incident, they must consider:

I. the seriousness or complexity of the incident

II. the possible outcomes of the investigation (administrative, disciplinary, civil or criminal)

III. if the incident requires referral to another agency or authority

IV. the resources required to conduct the investigation

V. who will conduct the investigation and what support they need

VI. the investigation process and timeframes

VII. the authorisation needed to undertake the investigation

VIII. the decision-makers and subsequent reporting obligations

62. It is recommended that, where possible, agencies apply the Australian Government Investigations Standards (AGIS) to maintain a minimum quality standard within investigations.

63. When investigating, the principles of procedural fairness should be applied, such that any individuals being investigated or whose interests could be adversely affected, should be informed of the case against them and given the opportunity to be heard by an unbiased decision-maker. Procedural fairness should also be applied to any actions taken as a result of the investigation, as well as when considering the security integrity of current or future investigations by the, or another agency.

## REPORTING SECURITY INCIDENTS

64. In some instances, a security incident must be reported to another agency or authority, depending on the nature and severity of the incident. Table 6 outlines the obligations to report particular security incidents, and to whom they must be reported. Non-reporting of an incident is considered a security incident.

[11] See the Public Interest Disclosure Act 2018 for more information.

### Table 6 – External reporting obligations

| Reportable incident | Agency obligation to report | Reportable to |
|---|---|---|
| **National security incidents** | Security incidents or situations that have, or could have, impact on national security,[12] including suspected:<br>- espionage<br>- sabotage<br>- politically motivated violence<br>- promotion of communal violence<br>- attacks on Australia's defence system<br>- acts of foreign interference<br>- serious threats to Australia's territorial and border integrity.[13]<br>Agencies **must** observe the need-to-know principle in relation to any details of a major security incident, until ASIO advises otherwise. | **Australian Security Intelligence Organisation**<br>Email: asa@asio.gov.au<br>Internet: http://www.asio.gov.au/<br>Phone: **13 ASIO (13 2746) (24hrs)**<br>For advice on if the incident needs to be reported, contact:<br>**National Security Hotline**<br>Phone: **1800 123 400** |
| **Cyber security incidents** | As per Premier and Cabinet Circular 042 – Cyber Security Incident Management, all agencies must report cyber security incidents to Cyber Security, Office of the Chief Information Officer.<br>Guidance on reporting cyber security incidents is available here. | **Cyber Security**<br>**Department of the Premier and Cabinet**<br>E: watchdesk@sa.gov.au<br>P: 1300 244 168 |
| **Significant security incidents** | As defined under Managing security incidents and listed in **Table** , significant security incidents **must** be reported to the SAPSF team in addition to all relevant authorities, or affected agencies.<br>Agencies are required to include significant security incidents in their annual security attestation (see SAPSF policy Annual security attestation for more detail). | **South Australian Protective Security Framework team**<br>Email: sapsf@sa.gov.au |

[12] As defined in the *Australian Security Intelligence Organisation Act 1979* (Cth)

[13] ASIO will assist agencies to conduct an initial assessment of any potential compromise and will either recommend the agency continue with its own investigation and advise of the outcome, or take over the investigation in close consultation with the agency

| Reportable incident | Agency obligation to report | Reportable to |
|---|---|---|
| **Personal Information Data Breaches** | Any inappropriate disclosure of personal information held by an agency, as governed by the Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions | **Privacy Committee of South Australia**<br>Phone: **(08) 8204 8786**<br>Email: StateRecords@sa.gov.au |
| **SA Cabinet material** | Any security incidents, suspected or actual, involving SA Cabinet material. The SA Cabinet Handbook contains guidance for handling of SA Cabinet material. | **Cabinet Office**<br>Contact: CabinetOffice@sa.gov.au |
| **Contact reporting** | Under the Australian Government Contact Reporting Scheme, employees are **required** to report a contact, either official or social, with or when:<br>• embassy or foreign government officials within Australia<br>• foreign officials and foreign nationals outside Australia<br>• contact seems suspicious, persistent or unusual in any respect, or becomes ongoing. Foreign officials could include trade or business representatives.<br>A person or group, regardless of nationality, seeks to obtain information they do not need to know for the responsibilities of their job. | **South Australian Security Officer**<br>**Department of the Premier and Cabinet**<br>Email: sapsf@sa.gov.au<br>DPC will then forward a Contact Report to ASIO via: cr@asio.gov.au |
| **Incidents involving security clearance holders** | In addition to the requirements for contact reporting, Security incidents involving security clearance holders **must** be reported to the Australian Government Security Vetting Agency (AGSVA) or the authorised vetting agency, at the appropriate time, of any incident that **may** affect a person's suitability to hold a security clearance. The appropriate time will depend on the incident, whether an investigation is ongoing and an assessment of personnel security risks.<br>When the employee is unsure about what should be reported, the employee should talk to their Agency Security Adviser, Manager, the South Australian Security | **South Australian Security Clearances**<br>Email: SASecurityClearances@sa.gov.au<br>Agency Security Adviser for your agency<br>The South Australian Security Officer will then provide notification to the **Australian Government Security Vetting Agency** via the<br>Security Officer Dashboard |

| Reportable incident | Agency obligation to report | Reportable to |
|---|---|---|
| | Clearance sponsor, or contact AGSVA. | |
| **Potential criminal/serious incidents** | Incidents that **may** constitute a criminal offence.<br>Depending on the type of offence, agencies **may** need to report to the Australian Federal Police (AFP) or to SAPOL.<br>See the AFP website for advice on the type of criminal incidents that are reported to Commonwealth or local police. | Local police for state or territory crimes<br>Phone: **13 14 44**<br>Crime Stoppers to anonymously provide information about a crime<br>Phone: **1800 333 000**<br>**AFP** for Commonwealth crimes<br>Internet: https://www.afp.gov.au<br>Phone: **02 6131 3000** |
| **Critical incidents involving public safety** | Critical incidents requiring immediate response, in particular where lives are at risk, agencies **must** call emergency services on **triple zero (000).**<br>Other critical incidents that **may** affect public safety and require a coordinated response from the South Australian and/or Commonwealth Governments **may** relate to:<br>• assault, including armed or military style assault<br>• arson, including suspected arson<br>• assassination, including suspected assassination<br>• bombing, including suspected use of explosive ordnance or improvised explosive devices<br>• chemical, biological or radiological attack, including suspected attacks<br>• attack on the National Information Infrastructure or critical infrastructure<br>• violent demonstration involving serious disruption of public order<br>• hijacking, including suspected hijacking | **Emergency services triple zero (000)**<br>**SAPOL**<br>Phone: **13 14 44**<br>Under South Australia's arrangements, the control agency designated for a critical incident **may** determine the circumstances warrant activation of the State Emergency Centre (SEC) and State Crisis Centre (SCC) arrangements. |

| Reportable incident | Agency obligation to report | Reportable to |
|---|---|---|
| | - hostage situation, including suspected hostage situation<br>- kidnapping, including suspected kidnapping<br>- mail bomb, including suspected mail bomb<br>- white powder incident, including real or significant hoax incidents. | |
| **Correspondence of security concern** | Correspondence received by an agency **may** be of a security concern if it contains:<br>- threats to use violence to achieve a political objective<br>- warning of imminent threats to specific individuals, groups, property or buildings | **SAPOL**<br>Phone: **13 14 44**<br>**Crime Stoppers** to anonymously provide information about a crime<br>Phone: **1800 333 000**<br>**National Security Hotline**<br>Phone: **1800 123 400** |
| **Incident affecting another agency** | Security incidents or unmitigated security risks that affect another agency's people, information or assets, particularly where agencies are co-located or are providing services to another agency. | **Accountable authority** of the agency whose people, information or assets **may** be affected. |
| **Security classified equipment and services** | Incidents involving Security Construction and Equipment Committee (SCEC) and ASIO approved destruction services | **SCEC**<br>Email: scec@scec.gov.au<br>Report: SCEC courier incident report |
| **Unauthorised foreign entity access to security classified information or assets** | Inappropriate or unauthorised sharing of security classified information or assets with a foreign national or international entity, without the protection of an agreement or arrangement (see SAPSF policy Security governance for international sharing) | **Agency ASEs**<br>In line with an internal agency reporting procedures, the incident may need to be externally reported, as per the other categories in this table. |
| **Compromise of foreign entity information or assets** | Failure to safeguard sensitive or security classified information of a foreign government or entity covered by an international agreement or arrangement. (see SAPSF policy Security governance for international sharing). | **Agency ASEs**<br>The agency **must** notify the originating foreign entity as soon as practicable. |

## SECURITY POLICY OR LEGISLATIVE REQUIREMENTS

65. The policies of the SAPSF have been developed to ensure consistency with other South Australian security policy and in accordance with relevant state and federal legislation. If the agency identifies any conflict between the requirements of the SAPSF or other relevant security policy or legislation, agencies must notify the SAPSF team.

66. Agencies must comply with all relevant security policy or legislative requirements in undertaking the requirements of the SAPSF.

67. Agencies are required to be aware of any agency-specific legislation that must be applied in carrying out official duties, and the requirements of the SAPSF do not override any legislative requirements or any other security policy requirements.

## SECURITY AWARENESS TRAINING

68. Security awareness training is a critical component of building an agency's security culture and overall security maturity.

69. Agencies must provide security awareness training to all employees upon commencement in the agency, and annually thereafter (via a security awareness refresher training), which outlines their agency-specific obligations and their responsibilities under the SAPSF. ASEs must determine the appropriate delivery method that ensures consistency across their agency for all employees, while ensuring all specific training or awareness requirements are met.

70. Employees in high-risk positions, positions of trust, security incident investigators or security clearance holders must be provided with specific security awareness training targeted to the scope and nature of their position.

71. Agency security plans should identify the most relevant areas of agency security that need to be addressed in the security awareness training.

72. Effective security awareness training is most effective when it:

    I. informs and regularly reminds employees of their individual and collective security responsibilities and how to raise issues or concerns

    II. ensures employees with specific security duties receive appropriate and up-to-date training

    III. briefs security cleared personnel on their access privileges and prohibitions attached to their security clearance level, either before being issued or during the renewal cycle

    IV. fulfils requirements for security clearance holders

## CONTENT OF SECURITY AWARENESS TRAINING

73. Table 7 provides the recommended content for security awareness training.

**Table 7 – Recommended content for security awareness training**

| Audience | Recommended content |
|---|---|
| **All personnel** | • overview of protective security requirements and arrangements within the agency<br>• description of the agency's security culture and security objectives<br>• personal safety and security measures in agency facilities and when working away from the office<br>• individual and line manager security responsibilities |

| Audience | Recommended content |
|---|---|
| | - training or updating information classification and protective marking requirements<br>- outlining the agency-specific security risks and threats and notifying of relevant SAPSF or agency-specific policies to address those risks and threats and the individual employee's responsibilities associated with them<br>- information control measures, such as need-to-know principle and security clearance requirements (if applicable)<br>- overseas travel safety and security responsibilities<br>- measures to identify and report unusual or suspicious behaviours<br>- asset (including information) protection<br>- reporting requirements and procedures, including<br>○ reporting security incidents (such as those listed in **Table 4 – Security incidents**)<br>○ contact reporting (including Contact Reporting Scheme)<br>○ reporting suitability concerns of other employees<br>○ any other agency-specific reporting requirements including public interest disclosures[14]<br>case studies of reported or investigated security incidents[15] |
| **Additional content for security cleared personnel** | - briefings or training to ensure security cleared personnel understand any day-to-day responsibilities and reporting obligations they have (see SAPSF policy Maintaining employee suitability)<br>- consultation with compartment owners for any personnel with access to Sensitive Compartmented Information. |
| **Additional content for specialist, high-risk, or positions of trust** | - security awareness training specific to address the risks related to the specific focus or scope of their work. Such positions **may** include:<br>○ sensitive or priority negotiations or policy work<br>○ responsibility for controlling access to valuable or attractive assets (including information)<br>○ working in remote or dangerous locations<br>○ being required to liaise or share information with foreign officials. |

## SECURITY AWARENESS REFRESHER TRAINING

74. ASEs must determine what form (e.g., in person, online), scope of coverage and content is required for the annual security training to meet the security needs of the agency, and the minimum requirements of the SAPSF.

75. The annual refresher training should consider the current threat or risk environment for the agency, the goals and objectives of agency security plans and any inadequacies of previous trainings or recurring security incidents.

[14] See *Public Interest Disclosure Act 2018*

[15] It is **recommended** that any case studies are redacted to maintain appropriate confidentialities.

## SECURITY SA TEAMS SITE

76. The Security SA Teams site is a platform to share and repurpose resource material in relation to security in SA Government including governance, personnel security, information security, physical security and cyber security.

77. The site is jointly managed by Office of the Chief Information Officer (OCIO) and Security, Emergency and Recovery Management in DPC. It is recommended that only ASEs, ASAs, ITSAs or staff with security responsibilities are given access to this site. In order to gain access to the site, email approval must be provided by your ASE, ASA or ITSA to cybersecurityOCIO@sa.gov.au or SAPSF@sa.gov.au with the name of the channel/s the staff member needs access to. Table 8 lists the channels within the Security SA Teams site and the recommended audience for each:

**Table 8 - Security SA Team channels**

| Audience | Description | Recommended Audience |
|---|---|---|
| **Cyber Security** | This channel is used to share and repurpose cyber security material. | • ASE<br>• ITSA (including Deputies)<br>• ASA (optional)<br>• Employees with cyber security responsibilities |
| **Governance** | This channel is used to share security governance advice and resources. | • ASE<br>• ASA (including Deputies)<br>• ITSA (including Deputies)<br>• Employees with security governance responsibilities (e.g., protective security committee members) |
| **Information Security** | This channel is used to share information security advice and resources. | • ASE<br>• ASA (including Deputies)<br>• ITSA (including Deputies)<br>• Employees with information security responsibilities (e.g., records management, Freedom of Information officers) |
| **Personnel Security** | This channel is used to share personnel security advice and resources. | • ASE<br>• ASA (including Deputies)<br>• Employees with personnel security responsibilities (e.g., Human Resources staff, Workplace Health & Safety (WHS) officers) |
| **Physical Security** | This channel is used to share physical security advice and resources. | • ASE<br>• ASA<br>• Employees with physical security responsibilities (e.g., facilities managers, WHS officers) |

## STRENGTHENING SECURITY AWARENESS

78. Agencies may implement other measures to strengthen the security awareness of employees, including:

    I. security campaigns that address ongoing agency security needs

    II. security instructions and reminders via electronic bulletins or publications, such as visual displays or posters

    III. incorporating protective security competencies into employee selection processes or performance management programs

    IV. drills and exercises.

## SECURITY EMAIL ADDRESS

79. To prevent agency security from becoming siloed, a monitored, generic security email address must be established for agency security-related matters, which can be monitored by ASEs, security advisers and other security personnel as required. This enables a greater flow of security related information within the agency while also creating a central contact in the agency for external communications with other agencies.

80. It is recommended that the agency's security email address:

    I. take the form (or similar):

        a. [agencyname].security@sa.gov.au, or

        b. [agencyname].ASE@sa.gov.au

    II. be monitored by appropriate security personnel in the agency, including the ASE and security advisers

    III. provided to the SAPSF team and other relevant agencies to facilitate collaboration and communication

81. If an agency is unable to create a generic email address for security-related matters and relies on an individual's email address, it is recommended that that email address be transferred to or monitored by other staff during extended periods of absence.

82. Agencies may establish multiple security-related email addresses if appropriate to control the flow of specific information, however, the main agency security address will be used for all SAPSF-related correspondence.

# 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 person: sapsf@sa.gov.au |

# CHANGE LOG

| Version | Date | Changes |
|---|---|---|
| 1.0 | 20/04/2020 | First issue of policy |
| 1.1 | 21/08/2020 | Definition of ‘personnel’ updated |
| 2.0 | 30/11/2022 | Definition of ‘Position of Trust’ added<br>Definition of ‘risk-based approach’ added<br>Security clearances for agency security personnel updated (para 11)<br>Advice for Incidents involving security clearance holders updated (Table 6)<br>Guidance added for Security SA team site (para 76-77, Table 8) |

SOUTH
AUSTRALIA

Government
of South Australia