South Australian Protective Security Framework

PERSEC 2

MAINTAINING EMPLOYEE SUITABILITY

SOUTH AUSTRALIA

Government of South Australia

CONTENTS

POLICY

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

Ensure the ongoing suitability of all employees

SUPPORTING REQUIREMENTS

4. To ensure the ongoing suitability of all employees, agencies[1] **must:**

   I. establish processes to maintain confidence that all employees remain suitable to hold their position

   II. ensure security cleared employees[2] comply with the minimum requirements of their clearance at all times

   III. share information of security concern with the appropriate authorities.

[1] This policy applies toall 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".

2 Including eligibility waivers and conditional security clearance holders

GUIDANCE

ASSESSING AND MANAGING ONGOING SUITABILITY

5. Each agency has a responsibility to ensure its information, people and assets are protected from deliberate and accidental compromise or harm. This is an enduring requirement based upon the likelihood that security circumstances can and do change.
6. People who are suitable at the time of employment or commencement in a role may face changes in circumstances, or develop new behaviours, that could result in an increased risk to security. Examples might include encountering financial or personal hardship, undertaking risky behaviours or simply becoming careless with their security responsibilities.
7. The mandatory and recommended pre-employment checks outlined in SAPSF policy Recruiting employees only help determine an employee's suitability when they are starting a role. Agencies **must** identify and establish processes that help continue to monitor employees for any changes that might affect their ongoing suitability and implement processes to manage any associated risks.

INSIDER THREAT

8. Insider threat is the risk of compromise to South Australian Government information and resources from an agency's employees who may, or may not, have authorised access. It can occur either deliberately or accidentally and result from a wide range of circumstances or motives.
9. Many people working inside the South Australian Government, including contractors, have privileged access to sensitive, and sometimes security classified, information, resources, and agency facilities. Compromise of sensitive or security classified information or resources could have significant consequences[3] for individuals, groups, agencies, or the government generally. Effective ongoing assessment can reduce the risk of insider threat from both malicious and unwitting parties.

EFFECTIVE ONGOING ASSESSMENT

10. Effective ongoing assessment encourages and facilitates reporting of security concerns, and regularly collates and assesses information to identify changes that may signal a potential security concern.
11. An agency's procedures for ongoing assessment **should** be determined through risk assessments that consider:

    I. the type of employee and employment (ongoing employees, temporary employees, security clearance holders etc.)

    II. their level of access to sensitive or security classified information and resources

    III. the agency's tolerance for security risks

    IV. any position specific risks

[3] For example, under the Code of Ethics for the South Australian Public Sector regarding Handling Official Information. Non-compliance with the professional conduct standards constitutes misconduct as defined by the *Public Sector Act 2009* and any employee who fails to comply may be liable to disciplinary action.

V. the individual's personal risk profile.

12. **Table 1** outlines the **required** and **recommended** procedures for agencies to assess and manage ongoing suitability of employees.[4]

Table 1 – Recommended and required processes for assessing ongoing suitability

Procedure	Uncleared employees	Security-cleared employees
Assess security performance	Required	Required
Periodic employment suitability checks	Required	Required
Security incident reporting and follow up	Required	Required
Annual security check	Recommended	Required
Contact reporting obligations	Recommended	Required
Collecting and assessing information on changes in circumstances	Recommended	Required
Annual review of eligibility waivers	Not applicable	Required (for waiver holders)
Specific clearance maintenance requirements	Not applicable	Required (for conditional clearance holders)
Positive vetting maintenance obligations in accordance with the SMSMP-PVG[5]	Not applicable	Required (for Positive Vetting clearance holders)

SECURITY PERFORMANCE

13. Agencies **must** address any known security concerns relevant to their employees. Supervisors and managers should discuss with employees any concerns or issues identified regarding the conduct or compliance to the security requirements of the SAPSF and any agency-specific policies.
14. If concerns are identified in an employee's security performance, it is recommended that the agency undertakes any appropriate or required employment suitability checks to help determine the person's suitability for ongoing access to South Australian Government information and resources.
15. Agencies are encouraged to include security requirements or considerations in employee role statements. This allows security to be discussed during performance management processes and opportunities can be identified to address gaps in a

[4] Although it is a requirement to undertake periodic employment suitability checks, agencies can determine the frequency and nature of those checks in line with the agency's risk tolerance and threat environment.
[5] The Sensitive Material Security Management Protocol – Positive Vetting Guidelines (SMSMP-SVG) contains the addition security maintenance requirements for Positive Vetting clearance holders. It is available to agency security personnel by request via the PSPF community on GovTEAMS.

person's security knowledge or capability and determine if any additional training to address these issues is needed.

16. If a position requires a security clearance, the accountable authority/Agency Security Executive (ASE) of an agency **must** provide authorisation to DPC[6] to commence a security clearance application.[7] For information on how to apply for a security clearance see Security Clearances or contact the State Security Officer via SASecurityClearances@sa.gov.au.
17. A security clearance holder's ability to maintain their clearance may be impacted by any security concerns. Supervisors and managers **must** report information that could affect a person's security clearance to their Agency Security Adviser (ASA) and the clearance sponsor who **must** provide this information to the vetting agency that issued the clearance i.e., the Australian Government Security Vetting Agency (AGSVA).
18. An agency's human resources unit may also be able to assist identify security concerns at a high-level across business areas (e.g., regular or unexplained absences) through routine business processes and reporting that could indicate personal issues that could lead to security concerns. Agencies **should** consider the need for procedures within their human resources areas to identify and report information that could be of relevance to security. This decision **should** be based on the agency's security risk assessments and guidance **should** be provided to assist human resources areas in managing these processes, when required.

PERIODIC EMPLOYMENT SUITABILITY CHECKS

19. Pre-employment screening checks are effective at determining a person's suitability at a point-in-time prior to employment. Agencies **should** periodically repeat any necessary or useful pre-employment screening checks over the period of a person's employment to help inform assessment of their ongoing suitability.
20. The frequency and nature of these suitability checks **should** be based upon the criteria outlined under Effective ongoing assessment.
21. In addition to the recommended pre-employment screening checks outlined in SAPSF policy Recruiting employees, **Table 2** lists some additional methods to assess ongoing suitability.

Table 2 – Additional methods to assess ongoing suitability

Check	Description
Updating personal particulars	Relevant changes in personal circumstances **may** include: • immediate relationship or family members • residential address/history • qualifications • memberships of clubs, associations or interest groups • employment history • overseas travel

[6] South Australia Police (SAPOL) is an authorised vetting agency and clearance sponsor of SAPOL employees for NV1 and NV2 level security clearances.

[7] For more guidance on security clearance sponsorship see SAPSF policy Recruiting Employees

	• ongoing contact with persons from other countries • updating on significant changes in circumstances (e.g., conflicts of interest, business arrangements) • recent criminal charges or convictions • any other changes relevant to the person's employment Where possible, changes to a person's circumstances or details **should** be verified independently.
Confirming adherence to, or completion of employment conditions	If conditions have been placed upon a person's employment, agencies **must** confirm if these conditions have been met as required (e.g., citizenship or security clearance etc.)

SECURITY INCIDENT REPORTING AND FOLLOW UP

22. Under SAPSF policy Security planning, agencies **must** establish processes and procedures to enable a proactive response to security incidents. This includes the ability to manage and record incidents, conduct investigations, monitor security performance, identify inadequacies and gaps in existing mitigations and detect new or evolving security risks.
23. At the employee level, frequent or recurring incidents involving one or more of the same people, regardless of the scale or type of individual incidents, could be relevant to assessing suitability to maintain access to South Australian Government information and resources.
24. Information of security incidents relating to security clearance holders **must** be reported to the agency's ASA and clearance sponsor who **must** provide this information to the vetting agency that issued the clearance. Security clearances in South Australia are sponsored by DPC [8] therefore information of security incidents **must** be reported to the State Security Officer via SASecurityClearances@sa.gov.au.

SECURITY CLEARANCE MAINTENANCE

25. It is a condition of all security clearances[9] that holders undertake an annual security check which addresses:
    I. the person's compliance with general security clearance obligations and any specific clearance maintenance obligations (conditions). General obligations include compliance with agency security procedures (including Security performance and Periodic employment suitability checks), including reporting:
        a. changes in circumstances (domestic, financial etc.)
        b. security incidents
        c. suspicious, ongoing, unusual or persistent contacts[10]
        d. completion of security awareness training

    II. any workplace behaviours of concern

[8] South Australia Police (SAPOL) is an authorised vetting agency and clearance sponsor of SAPOL employees.
[9] See PSPF policy Ongoing assessment of personnel
10 See paragraph 30. *Contact reporting obligations* for more detail

26. The annual security check provides an opportunity to discuss any security related matters or concerns and reinforce awareness and understanding of security obligations.
27. Supervisors and managers are well placed to conduct annual security checks due to their knowledge of their employees. Advice on conducting annual security checks should be sought from the agency's ASA.
28. In addition to the annual security check, agencies remain **responsible for** assessing the ongoing suitability requirements for all employees in line with agency employment processes.
29. Where an annual security check identifies something of security concern, this information **must** be reported to the agency's ASA and clearance sponsor who **must** provide this information to the vetting agency that issued the clearance.

CONTACT REPORTING OBLIGATIONS

30. Security clearance holders **must** report any contact with another person or group that they believe is suspicious, unusual, or persistent, or where ongoing contact with a foreign national has been established. Reporting details of such incidents assists to reduce the enduring risk of espionage against South Australian or Commonwealth Government agencies and entities.
31. Security clearance holders **must** report any such contact to their agency's ASE or ASA and the clearance sponsor. Under the **Australian Government Contact Reporting Scheme**, the ASE, ASA and the clearance sponsor (i.e., DPC) are responsible for providing details of the contact to the authorised vetting agency and the Australian Security Intelligence Organisation (ASIO) via cr@asio.gov.au.[11]
32. It is **recommended** that other agency employees also be encouraged to report any activity they deem fits the above description via the same processes.

CHANGES IN CIRCUMSTANCES

33. Changes in personal circumstances can impact upon a person's suitability to maintain access to South Australian or Commonwealth Government information and resources. The ability to identify changes in circumstances early can reduce or prevent larger problems from developing.
34. Changes in personal circumstances **may:**
    I. increase a person's vulnerability to coercion
    II. lead to deliberate breaches or security, fraud or corruption
    III. be used by foreign actors, commercial organisations, issue-motivated groups, criminal organisation or others to request or force a person into compromising government information or resources.
35. Security clearance holders **must** report changes in circumstances to their ASA and clearance sponsor, who **must** provide this information to the vetting agency that issued the clearance.
36. An agency's practices **should** encourage clearance holders to self-report changes in circumstances, and the agency **should** have effective procedures in place to collect, assess and manage any relevant changes or security risks.

[11] Further information on the Australian Contact Reporting Scheme, including a template Contact Report Form, can be found in the PSPF community on GovTEAMS.

37. See the AGSVA website for guidance on what changes in circumstance **must** be reported.

ANNUAL REVIEW OF ELIGIBILITY WAIVERS

38. All security clearance eligibility waivers **must** be reviewed annually and before a security clearance is revalidated. See SAPSF policy Recruiting employees for more detail on application for eligibility waivers.
39. Eligibility waivers are role-specific, non-transferable, finite and subject to review.
40. Supervisors and managers **must** be informed of the limitations and conditions of the security clearance. Relevant colleagues **must** also be informed.

SPECIFIC CLEARANCE MAINTENANCE REQUIREMENTS

41. Consistent with SAPSF policy Recruiting employees, conditional security clearances **may** be issued by AGSVA where concerns about a person's suitability are not sufficient to deny issuing the clearance. In such instances, conditions **may** be placed upon the security clearance which **must** be followed by the clearance holder. Non-compliance with any special conditions **must** be reported to the agency's ASA and the clearance sponsor, who **must** provide this information to the vetting agency that issued the clearance.
42. Agencies **must** put in place effective mitigations to manage any risks related to a conditional security clearance.

CLEARANCE HOLDERS ON SECONDMENT OR TEMPORARY ASSIGNMENT

43. Agencies **must** determine all security clearance requirements or arrangements for employees seconded, or on temporary assignment, prior to their commencement in the position.
44. Agencies **must** notify the clearance sponsor of the role change, and the expected duration of the secondment or temporary assignment, so that AGSVA can be notified.
45. Any information of security concern regarding the clearance holder **must** be shared between the relevant agencies to ensure any extant security risks can continue to be managed. This information **must** also be shared with the clearance sponsor.

SECURITY CLEARANCE REVALIDATIONS

46. Agencies **must** ensure all security clearance holders maintain their clearance for as long as their requirement to have one. AGSVA mandates that all security clearances are revalidated in full at set intervals, depending on the level of clearance.
47. The checks undertaken at revalidation **must** cover the period since the initial clearance or last revalidation. If periods of time are deemed uncheckable for vetting purposes, or where the vetting agency is unable to provide adequate assurance about a clearance holder, then an Eligibility waiver **may** be required. See SAPSF policy Recruiting employees for more detail on eligibility waivers.
48. Vetting agencies **should** provide sufficient notification to clearance holders of the revalidation date, to confirm whether the requirement for a security clearance still remains. As per SAPSF policy Recruiting employees, agencies **must** ensure that all positions requiring a security clearance are clearly identified, and that all employees occupying those roles have a valid clearance at the correct level. This requirement extends to circumstances where a security clearance holder's duties or role changes.

SHARING INFORMATION OF SECURITY CONCERN

49. Each agency can only make effective assessments of employee suitability based upon the information available. Authorised vetting agencies can only make appropriate determinations of an individual's suitability to hold a clearance if relevant information is effectively shared.
50. Developing a positive security culture within the agency is a critical step in enabling security-related information to be identified and shared before an issue escalates to a security incident (see SAPSF policies Security governance and Security planning for more information on security culture).
51. Agencies **must** report information of security concern to all appropriate authorities, which **may** include supervisors or managers, human resources units, or agency security employees such as the ASA. It **must** also include any other South Australian Government agencies[12] that may be affected.
52. If the information of security concern relates to a security clearance holder, agencies **must** report to both the clearance sponsor and the authorised vetting agency[13].
53. All information **must** be shared in accordance with the with the South Australian Information Privacy Principles (IPPS) Instruction (PC012).

[12] See SAPSF policy Security governance for information on reporting of security incidents and Employee separation for reporting obligations relating to employees.
[13] The authorised vetting agency **must** conduct a review of a person's suitability to maintain a clearance if information of security concern is reported. The process is known as review for cause. For more information, see the Review for cause section of the PSPF policy Ongoing assessment of personnel.

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

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	19/12/2022	Removed reference to security clearance fact sheet in 37 as will no longer be maintained

Government
of South Australia