South Australian Protective Security Framework

PERSEC 3

EMPLOYEE SEPARATION

SOUTH AUSTRALIA

Government of South Australia

Contents

POLICY

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:
    I. employees leaving an agency, via transfer to another agency, resignation from the public sector or end of contract
    II. those whose employment has been terminated for any reason[1]
    III. employees transferring either temporarily or permanently to another state, territory or Commonwealth Government agency
    IV. those taking extended leave [2]
3. This policy is to be applied in conjunction with South Australian Protective Security Framework (SAPSF) policies Recruiting employees and Maintaining employee suitability

CORE REQUIREMENT

Securely manage the separation of all employees

SUPPORTING REQUIREMENTS

4. To ensure the secure separation of all employees, agencies[3] must:
    I. remove access to South Australian Government information and resources
    II. ensure sponsorship of security cleared employees[4] is withdrawn or transferred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[5]

[1] 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.
[2] This policy does not define a period of time for where 'extended leave' applies. See Extended leave for more guidance.
[3] 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".
[4] Including eligibility waivers and conditional security clearance holders
[5] Depending on the level of concern this **may** include the ASE, clearance sponsor, authorised vetting agency or the Australian Security Intelligence Organisation (ASIO)

V. manage any residual risks following the individual's departure

GUIDANCE

SECURELY MANAGING SEPARATION OF EMPLOYEES

5. Depending on the circumstances, employees separating from an agency can increase the risk of compromise to the agency's information and resources. Appropriate and effective security management in an agency will ensure that all relevant security policies and legislative obligations are met.

6. In line with this, agencies should develop effective, risk-based procedures and processes to support the requirement to securely manage the separation of all employees.

REMOVING ACCESS TO INFORMATION AND RESOURCES

7. Once a person separates from their role or agency within the South Australian Government, their requirement for ongoing access to official information and resources also ceases.

8. Agencies must remove access to both physical facilities and resources, information and communication technology (ICT) systems, as well as recover any agency property they have (including devices, access cards, keys etc.).

9. It is recommended that agencies sequence the removal of access to ensure they maintain the ability to successfully remove all access that person may have had. Table 1 provides examples of actions that may be required, and the sequence they may be undertaken.

Table 1 - Actions that may be taken before and after employee separation

Stage	Action
Before separating	• Recover ICT equipment of physical assets that have been issued to employees (e.g., tablets, USB keys, mobile phones etc.) • Recover corporate credit cards • Recover any hardcopy material (originals and/or copies)
After separating	• disable access to ICT systems, including email, telephone, voicemail, Citrix, and any cloud accounts. Ensure any additional external access to systems has also been disabled • remove physical access to facilities and resources (including keys and access cards) • change or remove combinations or locks ((e.g., doors, safes or security containers) that the person had access to

10. If an agency allows transfer of ownership of ICT equipment to separating employees, or the use of personal devices for work purposes, agencies **must** ensure:

    I. any business-related documents are archived in accordance with the agency's records management procedures

    II. all agency information is removed, including access to any back-ups

III. all agency software applications are removed and access disabled

IV. if necessary, erase the content of the device's hard drive entirely.

MANAGING SECURITY CLEARANCES

11. All security clearances require sponsorship from an authorised entity to be deemed valid. Sponsorship is based upon the assessment that the employees involved are required to hold a valid security clearance based upon their role and responsibilities of that role.

REMOVING SPONSORSHIP

12. In South Australia, the Department of the Premier and Cabinet (DPC) sponsors all security clearances.[6] DPC will only maintain sponsorship of a security clearance where an agency's ASE continues to authorise the need for the clearance.

13. If a security clearance holder separates from an agency, the agency **must** notify the clearance sponsor and withdraw authorisation for sponsorship of that clearance. The clearance sponsor will then notify the authorised vetting agency who will amend the status[7] of the security clearance accordingly.

14. Agencies **must** advise the clearance sponsor if the separation is a result of any misconduct or security incident or concern. If other agencies **may** be impacted by these findings, ASEs from those agencies **should** also be notified.

TRANSFERRING SPONSORSHIP

15. If the separating person is transferring, either temporarily or permanently, to another South Australian agency, agencies **must** notify the clearance sponsor and, where possible, provide details of the transfer.

16. If the person is transferring outside of the South Australian Government, then agencies **must** notify the clearance sponsor that the sponsorship needs to be withdrawn. If the person still requires their security clearance for their new position, they and the receiving agency are responsible for ensuring the sponsorship is transferred to an appropriate authority.[8]

17. If an agency is receiving security cleared employees from another South Australian Government agency, the agency **must** notify the clearance sponsor as to whether sponsorship of the clearance is still required. If the clearance is still required, the ASE **must** provide authorisation to the clearance sponsor.

18. If an agency is receiving security cleared employees from outside the South Australian Government, the agency **must** ensure sponsorship of the security clearance is transferred to the appropriate South Australian clearance sponsor. Please see South Australian Security Clearances for more information.

TRANSFERRING PERSONAL SECURITY FILES

19. If a clearance holder transfers to another agency covered by a different authorised vetting agency, the personal security vetting file of the clearance holder **must** also be

[6] South Australia Police (SAPOL) is an authorised vetting agency and clearance sponsor of SAPOL employees for NV1 and NV2 level security clearances.
[7] PSPF policy Eligibility and suitability of personnel provides definitions of the statuses that are applied to security clearances.
[8] Authorised vetting agencies **must** only issue security clearances where it is sponsored by an Australian Government entity, or otherwise authorised by the Australian Government.

transferred to the new authorised vetting agency. Specific guidance for transferring personal security vetting files is available under PSPF policy Separating personnel.

ONGOING SECURITY OBLIGATIONS

20. All separating employees, whether departing temporarily or permanently, **must** be reminded of any ongoing security obligations they have associated with their former position.
21. People with access to sensitive or security classified information **must** be debriefed prior to separation. This **may** include if employees have ever been briefed into certain security caveats or compartments that have additional briefing/debriefing requirements.[9]
22. Separating employees also have ongoing obligations under various legislation[10] as well as information relating to intellectual property[11] and agencies **must** ensure separating employees are aware of these obligations.
23. Separating employees **should** also be reminded of their contact reporting obligations (see SAPSF policy Maintaining employee suitability).
24. It is **recommended** that agencies provide separating employees the opportunity to confidentially express any security concerns relating to agency procedures or colleagues prior to separation.

SHARING INFORMATION OF SECURITY CONCERN WITH ASES

25. There are potentially many stakeholders who may need to be made aware of information of security concern relating to an agency's employees. Agencies must ensure that all information sharing both within and within outside of the agency is consistent with the DPC Circular PC012 - Information Privacy Principles (IPPS) Instruction.

WITH ASEs

26. If an agency plans to terminate a person's employment on account of misconduct or security grounds, the agency's ASE or relevant security adviser **must** be notified. Agencies are **responsible for** implementing appropriate separation procedures which **should** be based upon a risk-assessment of the separation.

WITH OTHER AGENCIES

27. If any risk is identified to another agency's interests or their security procedures, agencies **must** notify the ASE of the affected agency as soon as practicable.

WITH NEW EMPLOYERS

28. If the separating person is transferring, either temporarily or permanently, to another state, territory or Commonwealth Government agency, agencies **must** provide the new agency with any relevant security information. This information **should** include the outcome of pre-employment and periodic employment suitability checks, and any security mitigations that **may** have been required during the employment.

---

[9] Access to some information is subject to additional security requirements, such as caveat or compartment briefings. As ongoing access to such information is strictly need-to-know, employees no longer requiring access must be debriefed by the caveat or compartment owner.

[10] For example, *Crimes Act 1914* and *Criminal Code Act 1995*

[11] Any intellectual property invented or created as a result an individual's employment will remain the property of the Crown, unless otherwise agreed in writing between the accountable authority and employee.

29. It is **recommended** that agencies recognise any pre-employment and periodic employment suitability checks that have already been undertaken where they meet the agency's requirements.

WITH THE CLEARANCE SPONSOR/AUTHORISED VETTING AGENCY

30. For any security clearance holders in an agency, any information of security concern to the clearance sponsor or the authorised vetting agency must be provided.
31. Information of security concern must be reported to enable a clearance holder's suitability to be assessed.
32. The clearance sponsor or authorised vetting agency may report information of security concern to ASIO where required.

MANAGING RESIDUAL RISKS

33. Sometimes, employees will depart agencies without undertaking or completing all required separation procedures. This could be due to illness, injury, or simply where the person refuses to participate.
34. In such circumstances, all of the other requirements of this policy must still be applied, where possible, such as removal of access to systems and facilities, or cancelling sponsorship of security clearances, if applicable.
35. For elements of the separation process that cannot be completed, agencies must undertake a risk assessment for any residual aspect to the individual's employment that have not been resolved. Any risks identified that fall outside an agency's risk tolerance must have appropriate mitigations applied.

EXTENDED LEAVE

36. Under this policy, separation includes employees taking extended leave. This policy does not define a period of time considered 'extended leave',[12] it is **recommended** that agencies take a risk-based approach to determine a period of 'extended leave' based on the risk tolerance and function of the agency and the nature of the role in question.
37. If the risk assessment determines the circumstances around the individual's plans for extended leave determines the risk is low enough, then application of this policy **may** not be required.

[12] Except for security clearance holders. If a security clearance holder goes on extended leave (greater than 6 months), they will have the status of their clearance changed to 'inactive'. The clearance can be made 'active' again by the clearance sponsor when the individual returns to work, and any required vetting updates have been undertaken.

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 Nov 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	Policy reviewed, no changes

Government
of South Australia