14 Separating personnel

A. Purpose

1. This policy details the processes to protect Australian Government people, information and assets when personnel permanently or temporarily leave their employment with an entity. Effectively managing personnel security includes ensuring departing personnel fulfil their obligations to safeguard Australian Government resources; this limits the potential for the integrity, availability and confidentiality of those resources to be compromised.

Separating personnel

Separating personnel include:

- personnel voluntarily leaving an entity
- those whose employment has been terminated for misconduct or other adverse reasons
- personnel transferring temporarily or permanently to another Australian Government entity (including machinery of government changes)
- those taking extended leave.

B. Requirements

B.1 Core requirement

Each entity must ensure that separating personnel:

a. have their access to Australian Government resources withdrawn, and
b. are informed of any ongoing security obligations.

2. International examples demonstrate that incidents of insiders compromising resources can occur after an individual has ceased employment. Therefore, separation measures are vital to limit these risks.

B.2 Supporting requirements

3. **Requirements 1** and **2** apply to all personnel; this includes security cleared personnel, non-security cleared personnel, contractors and third party individuals. **Requirement 3** applies more broadly and in certain circumstances. **Requirement 4** applies to security cleared personnel.

Supporting requirements for separating personnel

#	Supporting requirements
Requirement 1. Sharing security relevant information, debriefs and continuing obligations	Prior to personnel separation or transfer, entities **must:** a. notify the Chief Security Officer, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons b. debrief all separating personnel who have access to sensitive or security classified information, including advising them of their continuing obligations under the *Crimes Act 1914*, *Criminal Code* and other relevant legislation, and obtain the person's acknowledgement of these obligations c. for personnel transferring to another Australian Government entity, provide the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks, and d. report any security (as defined in the in the *Australian Security Intelligence Organisation Act 1979*) concerns to the Australian Security Intelligence Organisation (ASIO).
Requirement 2. Withdrawal of access	On separation or transfer, entities **must** remove personnel's access to Australian Government resources, including: a. physical facilities, and b. ICT systems.
Requirement 3. Risk assessment	Where it is not possible to undertake required separation procedures, entities **must** undertake a risk assessment to identify any security implications.
Requirement 4. Security clearance actions	Following the separation of security cleared personnel: a. sponsoring entities **must** advise the relevant authorised vetting agency of: i. the separation of a clearance holder, including any relevant circumstances (eg termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, and ii. any identified risks or security concerns associated with the separation, including as a result of **Requirement 3**. b. authorised vetting agencies **must**: i. manage and record changes in the security clearance status of separating personnel, including a change of sponsoring entity, and ii. transfer personal security files where a clearance subject transfers to an entity covered by a different authorised vetting agency, to the extent that their enabling legislation allows.

C. Guidance

4. Managing security risks relating to separating personnel relies on entities:
   a. identifying risks, see C.1 and C.4
   b. reminding personnel of their ongoing security obligations, see C.2
   c. ensuring access to entities resources is withdrawn for separating personnel, see C.3
   d. sharing relevant details of the separation with other entities, including vetting agencies, see C.1.
5. The PSPF policy: Management structures and responsibilities requires entities to develop and use procedures that ensure relevant security policy or legislative obligations are met. In line with that requirement, the Attorney-General's Department recommends entities have procedures for managing personnel security during separation. These procedures will vary depending on the personnel being separated, their access to sensitive and security classified resources and the entity's assessment of the security risk.

C.1 Sharing relevant information

6. **Requirement 1a** mandates that the entity's Chief Security Officer, or relevant security advisor, is notified of any proposed cessations of employment resulting from misconduct (eg termination for cause or resignations following concerning conduct). The Attorney-General's Department recommends that any security measures for staff whose employment has been terminated are based on a risk assessment. Security measures for high-risk personnel may include:
   a. immediate suspension of duties

b. immediate removal of all access to entity systems and facilities

c. escorting the person from the premises.

7. If separation is the result of an incident (or if an incident is uncovered during the separation process), advise other affected entities if their interests or security arrangements could be affected. This is consistent with the PSPF policy: Reporting on security that requires entities to report on security each financial year to other entities whose interest could be affected.

C.1.1 Sharing information on transfer

8. **Requirement 1c** mandates that when personnel are transferring to another entity, the losing entity must provide the gaining entity with relevant security information. Relevant security information includes the outcome of pre-employment screening checks and any periodic employment suitability checks, as well as concerns that were mitigated as part of the employment screening process. The Attorney-General's Department recommends that entities recognise pre-employment screening and any periodic employment suitability checks already conducted by the losing entity where they meet all entity requirements. For guidance, see the PSPF policies: Eligibility and suitability of personnel and Ongoing assessment of personnel.

C.1.2 Informing relevant authorised vetting agencies

9. **Requirement 4ai** mandates that entities advise the relevant authorised vetting agency of the separation or transfer of personnel who hold an Australian Government security clearance. This includes advising the authorised vetting agency that sponsorship has been withdrawn from the security clearance and, where it is known that an individual is transferring to another Australian Government entity, the details of the transfer. **Requirement 4aii** mandates that entities advise the vetting agency of any identified risks or security concerns associated with the separation, for example where:

   a. the individual's employment or contract is terminated for cause

   b. the individual was subject to a code of conduct investigation, whether completed or not

   c. the individual departed without a security debrief

   d. there are outstanding security issues, including any risks or issues identified through a risk assessment conducted in accordance with **Requirement 3**.

C.1.3 Security concerns and risks

10. **Requirement 1d** mandates that entities identify and report any security concerns to ASIO (security is defined in the in the *Australian Security Intelligence Organisation Act 1979*). An example of where this may be particularly relevant is when separating personnel do not adhere to requirements of this policy (eg those departing without having a security debrief). The Attorney-General's Department recommends that entities provide personnel with an opportunity to confidentially express any security concerns relating to procedures or colleagues prior to separation.

C.2 Ongoing obligations and security debriefs

11. Prior to separation, **Requirement 1b** mandates that entities debrief separating personnel who have access to sensitive or security classified information. This may include caveated and compartmented information where additional briefing requirements apply. The Sensitive Material Security Management Protocol (SMSMP) sets out the protection and handling requirements for caveated information. The SMSMP is available to entity security advisors.

12. **Requirement 1b** mandates that entities advise separating personnel of their continuing obligations under the *Crimes Act 1914*, *Criminal Code* and other relevant legislation, and obtain the person's acknowledgement of these obligations. This acknowledgement helps safeguard Australian Government resources and limit the potential for the integrity, availability and confidentiality of sensitive or security classified information to be compromised.

13. The Attorney-General's Department recommends that entities remind all personnel of their contact reporting responsibilities. These include reporting any contacts from former colleagues who show a

suspicious, persistent or unusual interest in their work or that of the entity. This also applies where personnel are travelling overseas.

C.3 Withdrawal of access to Australian Government resources

14. The **core PSPF requirement on separating personnel** mandates that entities ensure separating personnel have their access to Australian Government resources withdrawn. **Requirement 2** highlights the importance of removing access to both physical facilities and ICT systems, including any special access arrangements and non-standard ICT systems (eg administrator access, remote access, ASNET, TS networks).

15. The Attorney-General's Department recommends entities consider the sequencing of withdrawal of access to resources. **Table 1** provides an example of actions for entities to consider prior to, and on separation of, personnel.

Table 1 Recommended entity processes for withdrawing access prior to and on separation or transfer of all personnel

Stage	Actions
Prior to separation	a. recover ICT equipment or physical assets that are issued to personnel, in particular, any portable devices [Note i] b. recover any corporate credit cards c. recover any hardcopy material (both originals and copies).
On separation	a. disable access to the ICT systems, including but not limited to email, telephone voicemail, Citrix, dropbox and cloud accounts b. revoke physical access to facilities and retrieve keys and access cards c. change any combinations for locks (eg doors, safes or security containers) that the person had access to.

Table 1 notes:

[i] Where entities allow the transfer of ownership of ICT equipment to separating personnel, or where entities allow the use of personal devices for work purposes, the Attorney-General's Department recommends that:

- any business related documents are archived in accordance with entity records management procedures
- entity information is removed
- all entity software applications are removed
- if necessary, the entire content of the device's hard drive is erased.

C.4 Risk assessments

16. **Requirement 3** mandates that entities undertake a risk assessment to identify any security implications where personnel depart without undertaking required separation procedures. This could include personnel who suffer injury or illness and cannot continue working, personnel who separate while on leave, or personnel who refuse to undergo separation processes.

17. For personnel taking extended leave, the risk assessment might consider the purpose of the leave, any travel plans, the degree of ongoing contact between the entity and the individual during the leave and whether it is likely the individual may decide not to return from leave. This assessment can inform the entity's decision on whether to apply separation procedures prior to the commencement of extended leave. For guidance on personnel security for extended leave, see C.6.

C.5 Security clearance actions

18. **Requirement 4** sets out the roles and responsibilities of sponsoring entities and authorised vetting agencies for the separation of security cleared personnel. For guidance on the responsibilities of sponsoring entities (as mandated under **Requirement 4a**) see C.1.2. For guidance supporting **Requirement 4bi** (relating to managing and recording changes in a security clearance status), see C.5.1. See C.5.2 for guidance on personal security files (**Requirement 4bii)**.

C.5.1 Managing and recording security clearance status

19. **Requirement 4bi** mandates that authorised vetting agencies manage and record changes in separating personnel's security clearance status, including where there is a change of sponsorship.

20. The PSPF policy: Eligibility and suitability of personnel requires that a security clearance be sponsored by an Australian Government entity (or otherwise authorised by the Australian Government, for example, under an agreement with the states and territories) and can only be sponsored by one entity at a time. Vetting agencies may allow entities to register their interest in the clearance (ie contractors working for more than one entity, or secondees where both the home and host entities have an interest). The PSPF policy: Eligibility and suitability of personnel provides definitions of statuses that may apply to a clearance.

C.5.2 Personal security file

21. **Requirement 4bii** mandates that authorised vetting agencies transfer personal security files where a clearance subject transfers to an entity covered by a different authorised vetting agency (where enabling legislation allows). **Table** 2 identifies Attorney-General's Department-recommended actions to take in such cases.

Table 2 Recommended personal security file actions

Stage	Actions
Permanent transfer	**Actions for the gaining sponsoring entity** Before personal security file actions commence, the gaining sponsoring entity: a. identifies the level of security clearance required and whether the clearance subject has previously held a security clearance (including the entity that sponsored the previous clearance) b. obtains the clearance holder's consent to share information [Note i] where a current or previous clearance is identified c. requests permanent transfer of sponsorship of the security clearance. This will trigger the authorised vetting agency to commence permanent transfer of the personal security file.
	Actions for the gaining vetting agency Once it has received a request for the permanent transfer of a security clearance from the gaining sponsoring entity, the gaining vetting agency: a. requests the personal security file from the losing vetting agency [Note ii] b. confirms the information in the personal security file meets the requirements for the requested level of security clearance, or commences a new vetting process if the sponsoring entity requires a clearance that is higher than the clearance held c. identifies and addresses concerns or anomalies in the personal security file at the time of transfer, including determining whether the concerns or anomalies warrant a review for cause d. confirm the transfer of the personal security file with the sponsoring entity, including if further actions will be undertaken before the transfer of sponsorship can be finalised (ie sharing any concerns or conducting a review for cause).
	Actions for the losing vetting agency: The losing vetting agency: a. facilitates transfer of the personal security file as soon as practicable, following receipt of request from the gaining vetting agency [Note iii] b. seeks consent from clearance subjects prior to transferring and sharing personal security files.
Temporary transfer	Only transfer personal security files if necessary, for example: a. the position in the gaining sponsoring entity requires a higher security clearance b. the clearance expires during the transfer or secondment period.

Table 2 notes:

[i] For guidance on informed consent to share information relating to employment screening and security clearance vetting, see the PSPF policy: Eligibility and suitability of personnel. For guidance on informed consent to share information about ongoing suitability, see the PSPF policy: Ongoing assessment of personnel.

[ii] Some entities have legal restrictions on the transfer of personal security files. For example, the Department of Defence cannot transfer the personal security files of current and former Regular or Reserve Australian Defence Force personnel and ASIO can only transfer personal security files to other AIC entities. ASIO can only provide a statement of clearance to other vetting agencies. Psychological assessments may only be transferred to another appropriately qualified psychologist and only with the specific consent of the clearance holder.

[iii] In some instances it may not be possible to transfer personal security files immediately. This includes where personnel are still employed by the losing entity, are under investigation for a security breach or violation, are being revalidated, or are undergoing a review for cause.

22. Where a personal security file contains a National Police Check subject to no exclusions under the Commonwealth spent convictions scheme, the scheme requires entities ensure any previous recorded convictions are not spent and reference to any convictions that are spent are removed. For information, see the Privacy fact sheet 41: Commonwealth spent convictions scheme.

23. If the original National Police Check is not shared (as a result of Commonwealth spent convictions scheme requirements), the Attorney-General's Department recommends that the gaining vetting agency request a new National Police Check on transfer of the personal security file. This meets the requirements outlined in the PSPF policy: Eligibility and suitability of personnel.

24. Consistent with the PSPF policies: Eligibility and suitability of personnel and Ongoing assessment of personnel, where there are concerns transferring personal security files, vetting agencies will advise the sponsoring entity. The sponsoring entity can then make a risk-based decision on providing or continuing access to Australian Government resources.

25. Transferred personal security files may include information that has been previously collected (eg personal information or copies of supporting information). The Attorney-General's Department recommends the gaining authorised vetting agency not request this information again, unless there are concerns about the authenticity of the documents originally supplied. If electronic packs are used, information may be regathered electronically to populate the electronic record; this occurs at the next revalidation or review of the security clearance.

C.5.3 Temporary transfer or secondment

26. Entity processes for the sponsorship of security clearances (including associated responsibilities for assessment and management of ongoing suitability for clearance holders on temporary transfer or secondment) need to be:

    a. flexible to account for the diversity of timeframes and arrangements applicable to secondment and other temporary transfers

    b. negotiated between the home entity and host entity on a case-by-case basis.

27. The Attorney-General's Department recommends the losing sponsoring entity (the home entity), in consultation with the gaining sponsoring entity (the host entity) determine whether to treat a temporary transfer or secondment as a separation for the purpose of security clearance sponsorship. Relevant factors to consider include:

    a. the duration of the transfer or secondment and the level of access personnel will require to the home entity and host entity resources during the transfer or secondment

    b. whether the host entity requires a security clearance for the position at the same, higher or lower level than the home entity

    c. whether both entities use the same authorised vetting agency and if there is a need to transfer the clearance holder's personal security file.

28. If the host entity requires a higher level of clearance or the clearance expires during the period of the temporary transfer, the Attorney-General's Department recommends that the host entity's authorised vetting agency is responsible for the upgrade of the clearance.

C.6 Extended leave

29. The definition of separating personnel includes those taking extended leave. As such, the personnel security requirements of this policy apply, unless a risk assessment determines this is not necessary.

30. This policy does not define the period of time to which the term 'extended leave' applies. The Attorney-General's Department recommends that entities take a risk-based approach to determine the length of leave that constitutes 'extended leave' by considering an entity's risk profile and any specific risks associated with the position. Generally, a period of three months or longer may be considered as extended leave.

31. An example of an entity balancing security risks with other desired human resource outcomes could be where it chooses not to apply separation procedures to personnel on maternity or paternity leave, and

allows ongoing access to the entity's buildings, but suspending access to sensitive resources and administrative accounts for the period of leave.

32. Note, the PSPF policy: Eligibility and suitability of personnel states that, where a clearance holder does not maintain their security clearance for a period greater than six months due to long term absence from their role, the security clearance is considered inactive. The Attorney-General's Department recommends that entities advise the vetting agency to change clearances to inactive for personnel on extended absences based on their risk assessment. When clearance subjects return to work, the vetting agency can make the clearance active, if requested, after undertaking appropriate vetting updates.

33. The Attorney-General's Department encourages entities to include personnel security guidance on the following in their human resources or leave-related procedures:

    a. notifying relevant security advisors in advance of personnel commencing extended leave, as well as completing risk assessments if required

    b. considering and managing security issues before extended leave is approved, particularly if it is assessed as likely that personnel may decide not to return. Entities are encouraged to resolve any security issues before the leave commences

    c. reminding personnel on extended leave of their ongoing confidentiality obligations

    d. briefing personnel travelling overseas of their responsibilities, including the requirement to report suspicious, unusual or persistent contacts, as well as contact with foreign nationals that becomes ongoing

    e. advising the authorised vetting agency when a security clearance holder is taking extended leave and requesting the clearance status be changed to inactive

    f. ensuring recommencement procedures include changing the status of the security clearance and noting that the vetting agency may need to undertake vetting updates.

D. Find out more

34. For information regarding separation procedures for contractors, see the PSPF policy: Security governance for contracted goods and service providers.

D.1 Change log

Table 3 Amendments in this policy

Version	Date	Section	Amendment
v2018.0	DD MMM YYYY	Throughout	Not applicable. This is the first issue of this policy