Australian Government
Attorney-General's Department

PROTECTIVE SECURITY POLICY FRAMEWORK

Securing government business:

Protective security guidance for executives

www.protectivesecurity.gov.au

ISBN: 978-1-925593-13-6 (Print)
ISBN: 978-1-920838-56-0 (Online)

Contents

Directive on the security of government business

The Australian Government is committed to ensuring the secure delivery of Government business and continuing to build trust and confidence in our ability to engage with and manage protective security risks.

To achieve ongoing and effective delivery of Australian Government business, I expect accountable authorities[1] to meet the four security outcomes set out in the Protective Security Policy Framework.

Entities realise the Protective Security Policy Framework's outcomes by implementing the framework's requirements and using security measures proportionately to address their unique security risk environments.

Security is everyone's business and I encourage Australian Government personnel to develop a comprehensive understanding and appreciation of the importance of a positive security culture embedded across the entity.

The Australian Government, through my Department with oversight of the Government Security Committee, will continue to assess emerging security risks and develop and refine protective security policy that promotes efficient, secure delivery of Government business.

The Hon Mark Dreyfus KC MP

Attorney-General

1 Under the *Public Governance, Performance and Accountability Act 2013*, the accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over, the entity's operations.

Applicability of the Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) applies to non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) to the extent consistent with legislation.

The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the PGPA Act.

Non-government organisations that access security classified information may be required to enter into a deed or agreement to apply relevant parts of the PSPF for that information.

State and territory government agencies that hold or access Commonwealth security classified information apply the PSPF to that information consistent with arrangements agreed between the Commonwealth, states and territories.

Structure of the PSPF

The PSPF consists of:

PRINCIPLES	OUTCOMES	CORE REQUIREMENTS	GUIDANCE
These apply to every area of security. As fundamental values that represent what is desirable for all entities, security principles guide decision-making. There are five (5) protective security principles in the PSPF.	These outline the desired end-state results the government aims to achieve. Desired protective security outcomes relate to security governance, as well as information, personnel and physical security.	These articulate what entities **must** do to achieve the government's desired protective security outcomes. There are 16 core requirements in the PSPF. For each core requirement supporting requirements are intended to facilitate a standardised approach to security implementation across government.	Guidance material provides advice on how PSPF requirements can be delivered.

This document outlines the PSPF's principles, outcomes and all core and supporting requirements. Guidance material is available from the PSPF website at www.protectivesecurity.gov.au.

Executive functions under the PSPF

The accountable authority of a non-corporate Commonwealth entity is answerable to the responsible minister for the protection of their organisation's people, information and assets.

The Attorney-General has set out his expectations in the Directive on the Security of Government Business, which requires accountable authorities to apply the PSPF and promote protective security as part of their entity's culture.

Appropriate application of protective security by government entities ensures the operational environment necessary for confident and secure conduct of government business. Managing protective security risks proportionately and effectively enables entities to protect the Government's people, information and assets.

To support the accountable authority, the PSPF requires the appointment of a Chief Security Officer (at the Senior Executive Service level) who is responsible for security in the entity. The Chief Security Officer has oversight and is empowered to make decisions on all elements of protective security within the entity.

Australian Government
Attorney-General's Department

Protective Security Policy Framework

PRINCIPLES

Principles apply to every area of security. As fundamental values that represent what is desirable for all entities, security principles guide decision-making.

1. Security is everyone's responsibility. Developing and fostering a positive security culture is critical to security outcomes.
2. Security enables the business of government. It supports the efficient and effective delivery of services.
3. Security measures applied proportionately protect entities' people, information and assets in line with their assessed risks.
4. Accountable authorities own the security risks of their entity and the entity's impact on shared risks.
5. A cycle of action, evaluation and learning is evident in response to security incidents.

OUTCOMES

Outcomes outline the desired end-state results the government aims to achieve.

GOVERNANCE

Each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring: clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.

INFORMATION

Each entity maintains the confidentiality, integrity and availability of all official information.

PERSONNEL

Each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.

PHYSICAL

Each entity provides a safe and secure physical environment for their people, information and assets.

CORE REQUIREMENTS

Core requirements articulate what entities must do to achieve the government's desired protective security outcomes.

1 Role of accountable authority

The accountable authority is answerable to their minister and the government for the security of their entity.

The accountable authority of each entity must:

a) determine their entity's tolerance for security risks
b) manage the security risks of their entity, and
c) consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.

The accountable authority of a lead security entity must:

a) provide other entities with advice, guidance and services related to government security
b) ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security, and
c) establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.

2 Management structures and responsibilities

The accountable authority must:

a) appoint a Chief Security Officer (CSO) at the Senior Executive Service level[1] to be responsible for security in the entity
b) empower the CSO to make decisions about:
   i. appointing security advisors within the entity
   ii. the entity's protective security planning
   iii. the entity's protective security practices and procedures
   iv. investigating, responding to, and reporting on security incidents, and
c) ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.

3 Security planning and risk management

Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks. The security plan details the:

a) security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities
b) threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets
c) entity's tolerance to security risks
d) maturity of the entity's capability to manage security risks, and
e) entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

4 Security maturity monitoring

Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.

5 Reporting on security

Each entity must report on security each financial year to:

a) its portfolio minister and the Attorney-General's Department on:
   i. whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF
   ii. the maturity of the entity's security capability
   iii. key risks to the entity's people, information and assets
   iv. details of measures taken to mitigate or otherwise manage identified security risks
b) affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation, and
c) the Australian Signals Directorate in relation to cyber security matters.

6 Security governance for contracted goods and service providers

Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.

7 Security governance for international sharing

Each entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.

8 Sensitive and classified information

Each entity must:

a) identify information holdings
b) assess the sensitivity and security classification of information holdings, and
c) implement operational controls for these information holdings proportional to their value, importance and sensitivity.

9 Access to information

Each entity must enable appropriate access to official information. This includes:

a) sharing information within the entity, as well as with other relevant stakeholders
b) ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and
c) controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.

10 Safeguarding data from cyber threats

Each entity must mitigate common and emerging cyber threats by:

a) implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents:
   i. application control
   ii. patching applications
   iii. configure Microsoft Office macro settings
   iv. user application hardening
   v. restrict administrative privileges
   vi. patch operating systems
   vii. multi-factor authentication
   viii. regular backups
b) considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents need to be implemented to achieve an acceptable level of residual risk for their entity.

11 Robust ICT systems

Each entity must have in place security measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the *Australian Government Information Security Manual* when implemented into the operational environment.

12 Eligibility and suitability of personnel

Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).

Entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.

13 Ongoing assessment of personnel

Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.

14 Separating personnel

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.

15 Physical security for entity resources

Each entity must implement physical security measures that minimise or remove the risk of:

a) harm to people, and
b) information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

16 Entity facilities

Each entity must:

a) ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets
b) in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and
c) accredit its security zones.

For each core requirement supporting requirements are intended to facilitate a standardised approach to security implementation across government—these are outlined in the following pages.

1 Where an entity has fewer than 100 employees, the accountable authority may appoint their Chief Security Officer at the Executive Level 2 (EL2) providing the EL2 meets a number of requirements).

1 Role of accountable authority

This policy outlines the role and responsibilities of an accountable authority.[2]

Applicable sections of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act):

> **Section 21 Non-corporate Commonwealth entities (application of government policy)**
> The accountable authority of a Commonwealth entity **must** govern their entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government.
>
> **Section 15 Duty to govern the Commonwealth entity**
> (1) The accountable authority of a Commonwealth entity **must** govern the entity in a way that:
> (a) promotes the proper use and management of public resources for which the authority is responsible.

This policy establishes consistent, efficient and effective protective security measures across government. It forms the basis for protecting people, information and assets from security threats and supports continuous delivery of Australian Government business.

Core requirement

The accountable authority is answerable to their minister and the government for the security of their entity.

*The accountable authority of each entity **must**:*

a. *determine their entity's tolerance for security risks*
b. *manage the security risks of their entity, and*
c. *consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.*

*The accountable authority of a lead security entity **must**:*

a. *provide other entities with advice, guidance and services related to government security*
b. *ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security, and*
c. *establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.*

Supporting requirement

Supporting requirement for role of accountable authority

#	Supporting requirement
Requirement 1. Exceptional circumstances	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority: a. **may** vary application, for a limited period of time, consistent with the entity's risk tolerance b. **must** record the decision to vary in the annual report on security to the Attorney-General's Department and advise remedial action taken to reduce the risk to the entity.

Guidance

See Role of accountable authority at www.protectivesecurity.gov.au.

2 The accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over, the entity's operations.

2 Management structures and responsibilities

This policy describes the management structures and responsibilities that determine how security decisions are made in accordance with security practices. This provides a governance base for entities to protect their people, information and assets.

Effective management structures and responsibilities require people to be appropriately skilled, empowered and resourced. This is essential to achieving security outcomes.

Core requirement

*The accountable authority **must**:*

a. *appoint a Chief Security Officer (CSO) at the Senior Executive Service level to be responsible for security in the entity*
b. *empower the CSO to make decisions about:*
   i. *appointing security advisors within the entity*
   ii. *the entity's protective security planning*
   iii. *the entity's protective security practices and procedures*
   iv. *investigating, responding to, and reporting on security incidents, and*
c. *ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.*

Supporting requirements

Supporting requirements for management structures and responsibilities

#	Supporting requirements
Requirement 1. Security advisors	The CSO **must** be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.
Requirement 2. Security procedures	Entities **must** develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported, and c. relevant security policy or legislative obligations are met.
Requirement 3. Reporting security incidents	Entities **must** provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.
Requirement 4. Security training	Entities **must** provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.
Requirement 5. Specific training	Entities **must** maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.

Guidance

See Management structures and responsibilities at www.protectivesecurity.gov.au. [3]

3 Where an entity has fewer than 100 employees the accountable authority may appoint their Chief Security Officer at the Executive Level 2 (EL2), providing the EL2:
- reports directly to the accountable authority on security matters, and
- has the sufficient authority and capability to perform the responsibilities of the CSO role.

3 Security planning and risk management

This policy describes how entities establish effective security planning and can embed security into risk management practices. Security planning can be used to identify and manage risks and assist decision-making by:

a. applying appropriate controls effectively and consistently (as part of the entity's existing risk management arrangements)
b. adapting to change while safeguarding the delivery of business and services
c. improving resilience to threats, vulnerabilities and challenges
d. driving protective security performance improvements.

Core requirement

*Each entity **must** have in place a security plan approved by the accountable authority to manage the entity's security risks. The security plan details the:*

a. security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities
b. threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets
c. entity's tolerance to security risks
d. maturity of the entity's capability to manage security risks, and
e. entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

Supporting requirements

Supporting requirements for security planning and risk management

#	Supporting requirements
Requirement 1. Security plan review	The security plan (and supporting security plans) **must** be reviewed at least every two years. The review process **must** include how the entity will: a. determine the adequacy of existing measures and mitigation controls, and b. respond to and manage significant shifts in the entity's risk, threat and operating environment.
Requirement 2. Critical assets	Entities **must** identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources to support their core business.
Requirement 3. Risk steward	Entities **must** identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.
Requirement 4. Impact of risks	When conducting a security risk assessment, entities **must** communicate to the affected Commonwealth entity any identified risks that could potentially impact on the business of another entity.
Requirement 5. Threat levels	The security plan (and supporting security plans) **must** include scalable measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.
Requirement 6. Alternative mitigations	Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they **must** document the decision and adjust the maturity level for the related PSPF requirement.

Guidance

See Security planning and risk management at www.protectivesecurity.gov.au.

4 Security maturity monitoring

This policy describes how an entity monitors and assesses the maturity of its security capability and risk culture. This includes an entity's capability to actively respond to emerging threats and changes in its security environment, while maintaining the protection of its people, information and assets.

Core requirement

*Each entity **must** assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.*

Supporting requirement

Supporting requirement for security maturity monitoring

#	Supporting requirement
Requirement 1. Security maturity record	Entities **must** document and evidence their assessment of the entity's security maturity.

Guidance

See Security maturity monitoring at www.protectivesecurity.gov.au.

5 Reporting on security

This policy details the information entities are required to report under the Protective Security Policy Framework (PSPF) to provide assurance about their implementation of sound and responsible protective security practices and to identify security risks and vulnerabilities and the steps being taken to mitigate them. The policy describes how entities assess the maturity of their security capability, including by considering the entity's:

a. progress in achieving the PSPF governance, information, personnel and physical security outcomes

b. level of implementation and management of the PSPF core and supporting requirements

c. risk environment and tolerance for security risks

d. strategies and timeframes to manage identified and unmitigated risks, and

e. security risks to people, information and assets.

Reporting provides assurance that sound and responsible protective security practices are occurring. It also identifies security risks and vulnerabilities and the steps being taken to mitigate them.

Core requirement

*Each entity **must** report on security each financial year to:*

a. its portfolio minister and the Attorney-General's Department on:

i. whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF

ii. the maturity of the entity's security capability

iii. key risks to the entity's people, information and assets, and

iv. details of measures taken to mitigate or otherwise manage identified security risks

b. affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation, and

c. the Australian Signals Directorate in relation to cyber security matters.

Supporting requirement

Supporting requirement for reporting on security

#	Supporting requirements
Requirement 1. PSPF reporting model and template	Each entity **must** submit a report on security each financial year: a. through the PSPF online reporting portal for information up to PROTECTED or b. by submitting an offline reporting template for information classified higher than PROTECTED.
Requirement 2. Reporting security incidents	Each entity **must** report any significant or reportable security incidents at the time they occur to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement, and c. other affected entities. Table 3 provides detailed guidance on reporting security incidents.
Requirement 3. ASD cyber security survey	Each entity **must** complete the Australian Signals Directorate's annual cyber security survey.

Guidance

See Reporting on security at www.protectivesecurity.gov.au.

6 Security governance for contracted goods and service providers

This policy provides information about assessing and managing security risks that arise from procuring goods and services. While procurement offers benefits (eg scalability, elasticity, performance, resilience and cost efficiency), the security risks of procuring goods and services need effective management to reduce the likelihood of additional financial and non-financial costs to government.

This policy supports the Commonwealth Procurement Rules (the CPRs) that govern how entities procure goods and services. The rules seek to achieve value for money and consideration of the financial and non-financial costs and benefits.

Relevant Commonwealth Procurement Rules[4]

Relevant entities **must** establish processes for the identification, analysis, allocation and treatment of risk when conducting a procurement. The effort directed to risk assessment and management should be commensurate with the scale, scope and risk of the procurement. Relevant entities should consider risks and their potential impact when making decisions relating to value for money assessments, approvals of proposals to spend relevant money and the terms of the contract.

Relevant entities should consider and manage their procurement security risk in accordance with the Australian Government's Protective Security Policy Framework.

Core requirement

*Each entity is accountable for the security risks arising from procuring goods and services, and **must** ensure contracted providers comply with relevant PSPF requirements.*

CPRs Appendix B: Definitions states that a contract is 'an arrangement, as defined by s23(2) of the PGPA Act, for the procurement of goods and services under which relevant money is payable or may become payable. Note: this includes standing offers and panels'.

Supporting requirements

Balancing the effort directed to risk assessment and management with the scale, scope and risk of the procurement is important (eg the procurement of tables or chairs will have a relatively minor protective security effort). This is significant because procurement of goods and services does not transfer the operational risk from the Commonwealth. The supporting requirements help entities consider security risks when undertaking procurement and applying relevant PSPF requirements.

4 Commonwealth Procurement Rules paragraphs 8.2-8.3

Supporting requirements for security governance for contracted goods and service providers

#	Supporting requirements
Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities **must** put in place proportionate protective security measures by identifying and documenting: a. specific security risks to its people, information and assets, and b. mitigations for identified risks.
Requirement 2. Establishing protective security terms and conditions in contracts	Entities **must** ensure that contracts for goods and services include relevant security terms and conditions for the provider to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement, and c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.
Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities **must** put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and b. manage any changes to the provision of goods or services, and reassess security risks.
Requirement 4. Completion or termination of a contract	Entities **must** implement appropriate security arrangements at completion or termination of a contract.

Guidance

See Security governance for contracted goods and service providers at www.protectivesecurity.gov.au.

7 Security governance for international sharing

This policy details protections for valuable information and assets under international sharing agreements or arrangements to which Australia is a party.

These international agreements or arrangements also help to safeguard Australian information and assets when shared with foreign partners.

Legislative provisions on international sharing

Communicating, or making available, classified information with another country or foreign organisation could be considered espionage under the Criminal Code.

However, specific legislative provisions[5] authorise entities to share information internationally under arrangements made or directions given by the relevant minister.

Core requirement

*Each entity **must** adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.*

Supporting requirements

Supporting requirements for security governance for international sharing

#	Supporting requirements
Requirement 1. Sharing information with a foreign entity	a. When an entity shares sensitive or security classified Australian Government information or assets with a foreign entity there **must** be an explicit legislative provision, an international agreement or an international arrangement in place for its protection. b. The following limitations apply, even when an international agreement or international arrangement is in place: i. entities **must not** share Australian Government information bearing the Australian Eyes Only (AUSTEO) caveat with a person who is not an Australian citizen, and ii. entities, other than the Australian Signals Directorate (ASD), Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS), Department of Defence and Office of National Assessments **must** not share Australian Government information bearing the Australian Government Access Only (AGAO) caveat with a person who is not an Australian citizen.
Requirement 2. Safeguarding foreign information	Where an international agreement or international arrangement is in place, entities **must** safeguard sensitive or security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement.

A foreign entity includes a foreign government and foreign contractors (meaning any individual or legal entity entering into or bound by a classified contract and includes subcontractors).

Guidance

See Security governance for international sharing at www.protectivesecurity.gov.au.

5 For example, section 19 of the *Australian Security Intelligence Organisation Act 1979* allows for cooperation with authorities of other countries approved by the minister as being capable of assisting in the performance of ASIO's functions.

8 Sensitive and classified information

This policy details how entities correctly classify their information and adopt handling arrangements that guard against information compromise.

Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations:

- **Confidentiality** of information refers to the limiting of access to information to authorised persons for approved purposes.
- **Integrity** of information refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.
- **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.

A security classification (PROTECTED, SECRET and TOP SECRET) is only applied to information (or assets that hold information, such as laptops, USBs) if it requires protection because the impact of compromise of the information or asset would be high or above.

The requirements in this policy do not displace obligations imposed on entities through other policies, legislation or regulations, or by any other means.

Core requirement

*Each entity **must**:*

a. identify information holdings

b. assess the sensitivity and security classification of information holdings, and

c. implement operational controls for these information holdings proportional to their value, importance and sensitivity.

Supporting requirements

Supporting requirements help Australian Government entities maintain the confidentiality, integrity and availability of official information—including where the entity is the originator of information (the entity that initially generated or received the information).

Supporting requirements for sensitive and classified information

#	Supporting requirements
Requirement 1. Identifying information holdings	The originator **must** determine whether information being generated is official information (intended for use as an official record) and whether that information is sensitive or security classified.
Requirement 2. Assessing sensitive and security classified information	a. To decide which security classification to apply, the originator **must**: i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and ii. set the security classification at the lowest reasonable level. b. The originator **must** assess the information as OFFICIAL: Sensitive if: i. a security classification does not apply, and ii. compromise of the information's confidentiality may result in limited damage to an individual, organisation or government generally.

#	Supporting requirements					
				Sensitive information	Security classified information	
		UNOFFICIAL	OFFICIAL			
				OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	Compromise of information confidentiality would be expected to cause	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
		No damage. This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.
Requirement 3. Declassification	The originator **must** remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity **must not** remove or change information's classification without the originator's approval.						
Requirement 4. Marking information	The originator **must** clearly identify sensitive and security classified information, including emails, using applicable protective markings by: a. using text-based protective markings to mark sensitive and security classified information (and associated metadata), unless impractical for operational reasons b. if text-based protective markings cannot be used, using colour-based protective markings, or c. if text or colour-based protective markings cannot be used, applying the entity's marking scheme for such scenarios. Entities must document a marking scheme for this purpose and train personnel appropriately.						
Requirement 5. Using metadata to mark information	Entities **must** apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate sensitive or security classified information: a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property) b. for OFFICIAL: Sensitive information, apply the 'Dissemination Limiting Marker' property c. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.						
Requirement 6. Caveats and accountable material	a. Caveats **must** be marked as text and only appear in conjunction with a security classification. b. Entities **must** ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements. c. For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.						
Requirement 7. Storage	Entities **must** ensure sensitive and security classified information is stored securely in an appropriate security container for the approved zone in accordance with the minimum protection requirements set out in Annexes A to D.						
Requirement 8. Transfer	Entities **must** ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in Annexes A to D.						
Requirement 9. Disposal	Entities **must** ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to D. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.						

Guidance

See Sensitive and classified information at www.protectivesecurity.gov.au.

9 Access to information

The policy details security protections supporting entities' provision of timely, reliable and appropriate access to official information. Providing access to information helps develop new products and services, can enhance consumer and business outcomes and assists with decision-making and policy development.

Access to government information does not need to be limited for security purposes, except in select circumstances as identified in the requirements (primarily when sharing sensitive or classified information, or disclosing information outside government).

Core requirement

*Each entity **must** enable appropriate access to official information. This includes:*

a. sharing information within the entity, as well as with other relevant stakeholders

b. ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and

c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.

Supporting requirements

Supporting requirements for access to information

#	Supporting requirements
Requirement 1. Formalised agreements for sharing information and resources	When disclosing security classified information or resources to a person or organisation outside of government, entities **must** have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.
Requirement 2. Limiting access to sensitive and classified information and resources	To reduce the risk of unauthorised disclosure, entities **must** ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.
Requirement 3. Ongoing access to sensitive or classified information and resources	a. Entities **must** ensure that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level: **Security classified information** **PROTECTED** / **SECRET** / **TOP SECRET** **Personnel security clearance for ongoing access**: Baseline security clearance or above. / Negative Vetting 1 security clearance or above. / Negative Vetting 2 security clearance or above. Note i Some Australian office holders are not required to hold a security clearance. b. In addition, entities **must** ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner. Note ii Access to caveated material that involves a codeword requires a briefing and may require a Negative Vetting 1, Negative Vetting 2 level or Positive Vetting level security clearance as well as other additional requirements. For guidance, see the PSPF policy: Sensitive and classified information and supporting Security Caveats Guidelines.
Requirement 4. Temporary access to classified information and resources	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities **must**: a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person, or ii. up to a maximum of three months in a 12-month period b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) c. supervise all temporary access d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance, and e. deny temporary access to caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).
Requirement 5. Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities **must** implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.

Guidance

See Access to information at www.protectivesecurity.gov.au.

10 Safeguarding data from cyber threats

This policy describes how entities can mitigate common and emerging cyber threats. Cyber threats faced by the Australian Government commonly include:

- external adversaries who steal data
- ransomware that denies access to data, and external adversaries who destroy data and prevent systems from functioning
- malicious insiders who steal data
- malicious insiders who destroy data and prevent systems from functioning.

The most common cyber threat facing entities is external adversaries who attempt to steal data. Often these adversaries want access to systems and information through email and web pages. It is critical that entities safeguard the information held on systems that can receive emails or browse internet content.

The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) provides expert guidance to help entities mitigate cyber threats. While no single mitigation strategy, or set of mitigation strategies, is guaranteed to prevent a cyber security incident, the ACSC estimates many cyber security incidents could be mitigated by implementing eight essential mitigation strategies (known as the Essential Eight). These mitigation strategies are considered the baseline for cyber security. Each entity also needs to consider which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents they need to implement to protect their entity.

Core requirement

Each entity must mitigate common and emerging cyber threats by:

a. implementing the following Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents:
   i. application control
   ii. patching applications
   iii. configure Microsoft Office macro settings
   iv. user application hardening
   v. restrict administrative privileges
   vi. patch operating systems
   vii. multi-factor authentication
   viii. regular backups

b. considering which of the remaining Strategies to Mitigate Cyber Security Incidents you need to implement to protect your entity.

Supporting requirements

Supporting requirements help to safeguard information from cyber threats when engaging with members of the public online.

Supporting requirements for safeguarding information from cyber threats

#	Supporting requirements
Requirement 1. Transacting online with the public	Entities **must** not expose the public to unnecessary cyber security risks when they transact online with government.

Guidance

See Safeguarding information from cyber threats at www.protectivesecurity.gov.au.

11 Robust ICT systems

This policy describes how entities can safeguard information and communication technology (ICT) systems to support the secure and continuous delivery of government business. Secure ICT systems protect the integrity (and facilitate the availability) of the information that entities process, store and communicate.

Core requirement

*Each entity **must** ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual's cyber security principles during all stages of the lifecycle of each system.*

Supporting requirements

Supporting requirements for robust ICT systems

#	Supporting requirements
Requirement 1. Authorisation of ICT systems to operate	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation. When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate must be based on the Information Security Manual's six step risk-based approach for cyber security.
Requirement 2. Gateways	Entities **must** protect internet-connected ICT systems, and the information and data they process, store or communicate, by implementing a gateway consistent with the Information Security Manual and the Digital Transformation Agency's Gateways policy.
Requirement 3. Hosting Certification Framework	Entities **must** ensure the secure hosting of sensitive and classified government information and data through the use of certified services and associated infrastructure by applying the Digital Transformation Agency's Hosting Certification Framework (HCF).
Requirement 4. Vulnerability Disclosure Program	Entities **must** have in place a vulnerability disclosure program.

Guidance

See Robust ICT systems at www.protectivesecurity.gov.au.

12 Eligibility and suitability of personnel

This policy details the pre-employment screening processes and standardised vetting practices to be undertaken when employing personnel and contractors. These processes provide a high-quality and consistent approach to managing personnel eligibility and suitability risk across government.

Core requirement

*Each entity **must** ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).*

*Entities **must** use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.*

Pre-employment screening is the primary activity used to mitigate an entity's personnel security risks. Entities may use security clearances where they need additional assurance of the suitability and integrity of personnel. This could be for access to security classified information, or to provide greater assurance for designated positions.

Supporting requirements

The supporting requirements clarify conditions for pre-employment screening and security clearances. This includes outlining the respective responsibilities of sponsoring entities and authorised vetting agencies in relation to security clearances.

Supporting requirements for eligibility and suitability of personnel

#	Supporting requirements
Requirement 1. Pre-employment screening	Entities **must** undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm.
Requirement 2. Security clearances	Entities **must**: a. identify and record positions that require a security clearance and the level of clearance required b. ensure each person working in an identified position has a valid security clearance issued by an authorised vetting agency c. before seeking a security clearance, confirm that the person meets pre-employment screening requirements Note i and is an Australian citizen d. if the person is not an Australian citizen and has a valid visa with work rights, provide the authorised vetting agency with an eligibility waiver by: i. establishing an exceptional business requirement and conducting a risk assessment, and ii. asking the accountable authority to consider and accept the risk of waiving the citizenship requirement Note ii e. if the authorised vetting agency assesses that the person has an uncheckable background, provide the vetting agency with an eligibility waiver by: i. establishing an exceptional business requirement and conducting a risk assessment (including seeking the advice of the vetting agency), and ii. asking the accountable authority to consider and accept the risk of waiving the checkable background requirement. Note iii

#	Supporting requirements
Requirement 3. Personnel security vetting standard	Authorised vetting agencies **must**: a. only issue a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government b. seek informed consent from the clearance subject to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance c. assess the clearance subject's suitability to hold a security clearance by: i. considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines ii. for TOP SECRET-Privileged Access security clearances, assessing their trustworthiness and commitment to Australia, its values and its democratic system of government (i.e. honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the TOP SECRET-Privileged Access Standard Note iv iii. conducting minimum personnel security checks for a security clearance outlined below and iv. resolving any doubt in the national interest.

Minimum personnel security checks

Check	Security Clearance Level				
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**	**TOP SECRET-Privileged Access** note v
Verification of identity	✓required.	✓required.	✓required.	✓required.	✓required.
	Entities must verify the person's identification documents with the issuing authority by using the Document Verification Service for Australian issued primary identification documents.				
Confirmation of Australian citizenship and status of any other citizenships	✓required.	✓required.	✓required.	✓required.	✓required.
Background check	✓Required for the checkable period of 5 years.	✓Required for the checkable period of 10 years.	✓Required for the checkable period of 10 years.	✓Required for the checkable period that is greater of 10 years or from the age of 16.	✓Required for the checkable period that is from the age of 16, or 10 years if under 26 years of age.
Official secrets declaration	✓required.	✓required.	✓required.	✓required.	✓required.
Statutory declaration	✓required.	✓required.	✓required.	✓required.	N/a
Referee checks	✓required.	✓required.	✓required.	✓required.	✓required.
Digital footprint check	✓required.	✓required.	✓required.	✓required.	✓required.
National police check/criminal history check	✓required, no exclusion.	✓required, full exclusion.	✓check required, full exclusion.	✓required, full exclusion.	✓required.
Financial history assessment	✓ required.	✓required.	✓ required.	✓required.	N/a
Financial statement	Not required.	✓ required.	✓ required.	✓required with supporting documents.	N/a

#	Supporting requirements				
	Financial probity assessment	Not required.	Not required.	Not required.	✓required.	N/a
	ASIO assessment	Not required.	✓required.	✓required.	✓required.	✓required.
	Security interview	Not required.	Not required.	✓required.	✓required.	✓required.
	Psychological security assessment	Not required.	Not required.	Not required.	✓required.	✓required.
	Overseas travel check	N/a	N/a	N/a	N/a	✓required.
Requirement 3. Personnel security vetting standard *cont.*	d. if a clearance subject has an uncheckable background: v. provide the sponsoring entity with information to inform a risk assessment, and vi. only issue a clearance if the accountable authority waives the checkable background requirement (see **Requirement 2e**) e. if security concerns are identified during the vetting or security assessment process that are not sufficient to deny a security clearance, and the related risks can be managed through conditions attached to the security clearance: vii. identify the conditions and any specific clearance maintenance requirements viii. provide the sponsoring entity with information about the security concerns to inform a risk assessment, and ix. only issue a conditional clearance if the accountable authority and the clearance subject accept the clearance conditions [Note vi] f. if any other relevant information of security concern is identified during the vetting process, provide the sponsoring entity with information to inform a risk assessment when advising them of the outcome of the security vetting process [Note vii] g. without compromising the national interest, apply the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny a security clearance (including grant lower level) or grant a conditional security clearance,[Note viii] and h. ensure all vetting personnel attain and maintain the required skills and competencies for their role.				

Supporting requirements notes:

i An exception applies for entities authorised as vetting agencies for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearances.

ii The accountable authority may delegate this decision to the Chief Security Officer.

iii The accountable authority may delegate this decision to the Chief Security Officer.

iv The TOP SECRET-Privileged Access Standard contains specific guidance on the TOP SECRET-Privileged Access process. The TOP SECRET-Privileged Access Standard is available to TOP SECRET-Privileged Access practitioners and Chief Security Officers via the TOP SECRET-Privileged Access Quality Assurance Office.

v The TOP SECRET-Privileged Access Standard contains specific guidance on the minimum personnel security checks for TOP SECRET-Privileged Access security clearances.

vi The accountable authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the accountable authority of the clearance conditions.

vii Where security concerns are identified that may lead to an adverse recommendation, the vetting agency (while any determination is still pending, including where a clearance subject has been invited to respond to identified risks) shares only relevant information with the sponsoring entity to enable temporary mitigations until a final outcome is made. See Requirement 3g.

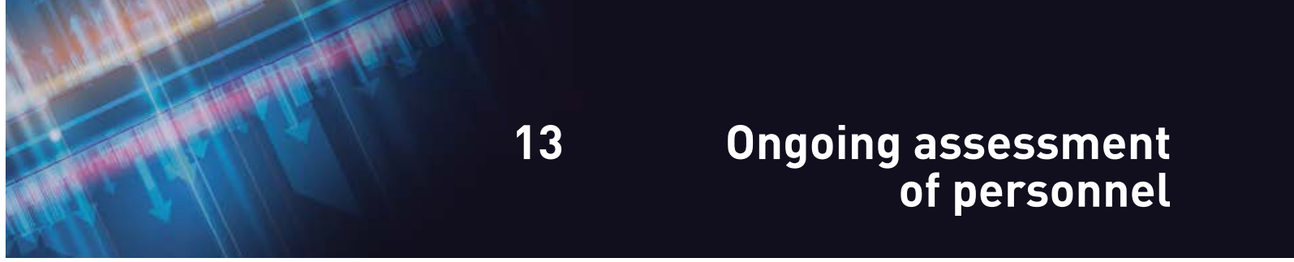
viii Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security assessment.

Requirement 1 applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources.[6] **Requirements 2** and **3** apply to security cleared personnel only

Guidance

See Eligibility and suitability of personnel at www.protectivesecurity.gov.au.

6 Requirements 1 and 2c do not apply to the staff of Ministers employed under Part III of the *Members of Parliament (Staff) Act 1984*. For further information, see Annex A of PSPF policy: Ongoing assessment of personnel.



13 Ongoing assessment of personnel

This policy describes how entities maintain confidence in their personnel's ongoing suitability to access Australian Government resources, and manage the risk of malicious or unwitting insiders. It is critical that entities are aware of changes in their employees' circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility.

Effectively assessing and managing ongoing suitability ensures that entities' personnel, including contractors, continue to meet eligibility and suitability requirements established at the point of engagement. This includes continuing to meet an appropriate standard of trustworthiness and commitment to Australia.

Core requirement

*Each entity **must** assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.*

Accountable authorities are responsible for determining their entity's risk tolerance and managing the security risks of their entity, including as they relate to the ongoing suitability of personnel to access Australian Government resources.

Sponsoring entities and authorised vetting agencies play a critical role in assuring ongoing suitability of personnel occupying positions that require access to security classified resources, or additional levels of assurance. The supporting requirements detail sponsoring entities' and vetting agencies' respective responsibilities for assessing the ongoing suitability of security cleared personnel.

Supporting requirements

Supporting requirements for ongoing assessment of personnel

#	Supporting requirements
Requirement 1. Security clearance maintenance Note i	a. Sponsoring entities **must** actively monitor and manage the ongoing suitability of their security cleared personnel, including: i. collecting, assessing and sharing information of security concern ii. conducting annual security checks with all security cleared personnel iii. monitoring compliance with, and managing risk in relation to, clearance maintenance requirements for security clearance holders granted a conditional security clearance and reporting non-compliance to the authorised vetting agency iv. reviewing eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer v. implementing the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged access security clearances. vi. assisting the authorised vetting agency to review the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause).. b. Vetting agencies **must**: i. share information of security concern about security clearance holders with sponsoring entities ii. ii.assess and respond to information of security concern about security clearance holders, which includes reports from sponsoring entities iii. for conditional security clearances, review conditions annually iv. review the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause), and v. implement the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.

#	Supporting requirements
Requirement 2. Security clearance revalidation	Vetting agencies **must** reassess a clearance holder's suitability to hold a security clearance by: a. for Baseline, Negative vetting 1, Negative Vetting 2 and Positive Vetting security clearances, considering their trustworthiness and commitment to Australia, its values and its democratic system of government (ie honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the Personnel Security Adjudicative Guidelines (see the PSPF policy: Eligibility and suitability of personnel Annex A) b. for TOP SECRET-Privileged Access security clearances, assessing their trustworthiness and commitment to Australia, its values and its democratic system of government (ie honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the TOP SECRET-Privileged Access Standard [Note ii] c. revalidating minimum personnel security checks for a security clearance outlined below, and d. resolving any doubt in the national interest.

Minimum requirements for revalidation of security clearances

Check	Security Clearance Level				
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**	**TOP SECRET-Privileged Access**[note iii]
Revalidation [Note iv] undertaken at least every:	15 years.	10 years.	5 to 7 years.	5 to 7 years.	7 years.
Updated personal particulars	✓required.	✓required.	✓required.	✓required.	✓required.
	Entities **must** confirm any changes to a clearance holder's personal particulars using identification documents verified with the issuing authority by using the Document Verification Service for Australian issued primary identification documents.				
Background assessment covering period since the initial clearance or last revalidation	✓required.	✓required.	✓required.	✓required.	✓required.
Referee checks covering period since the initial clearance or last revalidation	✓required.	✓required.	✓required.	✓required.	✓required.
Digital footprint check covering period since the initial clearance or last revalidation	✓required.	✓required.	✓required.	✓required.	✓required.
National police check/criminal history check	✓Required, full exclusion	✓Required, full exclusion	✓Required, full exclusion	✓Required, full exclusion	✓Required, full exclusion
Financial history assessment	✓check required.	✓check required.	✓required.	✓required.	N/a
Financial statement	Not required.	✓ required.	✓required.	✓Required with supporting documents.	N/a

#	Supporting requirements

Check	Security Clearance Level				
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**	**TOP SECRET-Privileged Access**[note v]
Financial probity assessment	Not applicable, check not required.	Not applicable, check not required.	Not applicable, check not required.	✓required.	
ASIO assessment	Not required.	✓required.	✓required.	✓required.	
Security interview	Not required.	Not required.	✓required.	✓required.	
Psychological assessment	Not required.	Not required.	Not required.	✓required.	
Overseas travel check	N/a	N/a	N/a	N/a	✓required.

Supporting requirements notes:

i Additional security clearance maintenance for Positive Vetting clearance holders are contained in the Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (SMSMP-PVG). The SMSMP-PVG is available to entity security advisors or upon request via the PSPF community on GovTEAMS. Additional security clearance maintenance for TOP SECRET-Privileged Access security clearance holders is contained in the TOP SECRET-Privileged Access Standard, available to TOP SECRET-Privileged Access practitioners and sponsoring entity Chief Security Officers via the TOP SECRET-Privileged Access Quality Assurance Office.

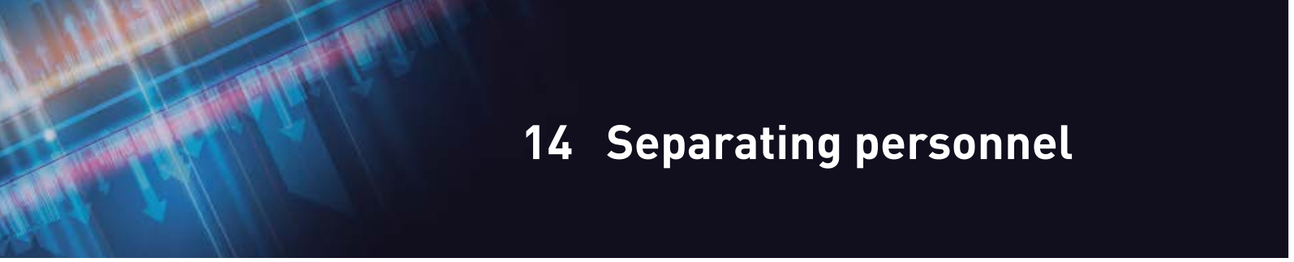
ii The TOP SECRET-Privileged Access Standard contains specific guidance on the TOP SECRET-Privileged Access process. The TOP SECRET-Privileged Access Standard is available to TOP SECRET-Privileged Access practitioners and sponsoring entity Chief Security Officers via the TOP SECRET-Privileged Access Quality Assurance Office.

iii The TOP SECRET-Privileged Access Standard contains specific guidance on the minimum personnel security checks for the revalidation of TOP SECRET-Privileged Access security clearances.

iv A revalidation covers the period since the initial clearance or last revalidation was completed, unless there are significant security concerns that raise doubts about the previous assessment, or indication of an enduring pattern of behaviour.

Guidance

See Ongoing assessment of personnel at www.protectivesecurity.gov.au.



14 Separating personnel

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.

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.

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.

Supporting requirements

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 *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.

Guidance

See Separating personnel at www.protectivesecurity.gov.au.

15 Physical security for entity resources

This policy describes the physical protections required to safeguard people (consistent with the requirements of the *Work Health and Safety Act 2011)*, information and assets (including ICT equipment) to minimise or remove security risk.

Core requirement

*Each entity **must** implement physical security measures that minimise or remove the risk of:*

a. *harm to people, and*

b. *information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.*

Supporting requirements

The supporting requirements help entities identify the resources that need protection and the level of physical security measures required to protect resources appropriately.

Supporting requirements for physical security for entity resources

#	Supporting requirements
Requirement 1. Physical security measures	Entities **must** put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise,[Note i] loss or damage.
Requirement 2. Security containers, cabinets and rooms	Entities **must** assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.
Requirement 3. Disposal	Entities **must** dispose of physical assets securely.

Supporting requirement notes:

Note i Information is compromised as defined in the PSPF policy: Sensitive and classified information, Table 1.

Guidance

See Physical security for entity resources at www.protectivesecurity.gov.au.

16 Entity facilities

This policy provides the consistent and structured approach to be applied to building construction, security zoning and physical security control measures of entity facilities. This ensures the protection of Australian Government people, information and physical assets secured by those facilities.

Core requirement

*Each entity **must**:*

a. *ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets*

b. *in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and*

c. *accredit its security zones.*

Supporting requirements

The supporting requirements help entities consider physical security controls for entity facilities and apply relevant PSPF requirements.

Supporting requirements for entity facilities

Requirement 1. Design and modify facilities

When designing or modifying facilities, entities **must**:

a. secure and control access to facilities to meet the highest risk level to entity resources, and

b. define restricted access areas as detailed below.

Zone name	Zone definition
Zone One	Public access
Zone Two	Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.
Zone Three	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control.
Zone Four	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control.
Zone Five	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control.

#	Supporting requirements
Requirement 2. Building construction	Entities **must** ensure: a. facilities for Zones Two to Five that store sensitive or security classified information and assets are constructed in accordance with applicable sections of: i. ASIO Technical Note 1/15—Physical Security Zones, and ii. ASIO Technical Note 5/12—Physical Security Zones (TOP SECRET) areas. b. security zones are constructed to protect against the highest risk level in accordance with the entity security risk assessment in areas: i. accessed by the public and authorised personnel, and ii. where physical assets, other than sensitive and security classified assets, are stored.
Requirement 3. Hardware	Entities **must**, in areas that store sensitive and security classified information, ensure perimeter doors and hardware are: a. constructed in accordance with ASIO Technical Notes in Zones Two to Five, and b. secured with SCEC-approved products rated to Security Level 3 in Zones Three to Five.
Requirement 4. Security alarm systems	Entities **must**: a. for Zone Three, use either: i. a Type 1 security alarm system,[Note i] or ii. a Class 5 commercial security alarm system, or iii. guard patrols performed at random intervals and within every four hours b. for Zone Four and Zone Five, use: i. a SCEC-approved Type 1A or Type 1 security alarm system in accordance with the Type 1A security alarm system transition policy [Note i] with SCEC-approved detection devices, and ii. a SCEC-endorsed Security Zone Consultant to design and commission the SCEC-approved Type 1A alarm system c. in Zones Three [Note ii] to Five: i. use sectionalised security alarm systems ii. security alarm systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. monitored and responded to in a timely manner, and iii. privileged alarm systems operators and users are appropriately trained and security cleared.

#	Supporting requirements
Requirement 5. Access control	a. Entities **must** control access to Zones Two to Five within the entity's facilities by only allowing access for authorised personnel, visitors, vehicles and equipment and apply the following controls: i. for Zones Two to Five, use: A. electronic access control systems where there are no other suitable identity verification and access control measures in place ii. for Zones Three to Five, use: A. identity cards with personal identity verification B. sectionalised access control system with full audit C. regular review of audit logs for any unusual or prohibited activity iii. for Zone Four and Zone Five, ensure access control systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. privileged operators and users are appropriately trained and security cleared to the level of the security zone, and iv. for Zone Five, use dual authentication access control. b. When granting ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, the entity's accountable authority or CSO **must** ensure the person has: i. the required level of security clearance for the facility's security zones, and ii. a business need supported by a business case and risk assessment, which is reassessed on a regular basis at least every two years.
Requirement 6. Technical surveillance counter-measures	Entities **must** ensure a technical surveillance countermeasures inspection is completed for facilities where: a. TOP SECRET discussions are regularly held, or b. the compromise of discussions may have a catastrophic business impact level.
Requirement 7. Security zone certification	CSOs or delegated security advisers **must**, before using a facility operationally: a. certify the facility's Zones One to Four in accordance with the PSPF and ASIO Technical Notes b. for Zone Five facilities, obtain: i. ASIO-T4 physical security certification for security areas used to handle TOP SECRET sensitive and security classified information, sensitive compartmented information (SCI) or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level.

#	Supporting requirements
Requirement 8. Security zone accreditation	CSOs or delegated security advisers **must**, before using a facility operationally: a. accredit Zones One to Five when the security controls are certified and the entity determines and accepts the residual risks, and b. for Zone Five facilities, obtain: i. Australian Signals Directorate security accreditation for areas used to secure and access TOP SECRET sensitive compartmented information.
Requirement 9. ICT facilities	Entities **must**: a. certify and accredit the security zone for ICT sensitive and security classified information with an extreme business impact level b. ensure that all TOP SECRET information ICT facilities are in compartments within an accredited Zone Five area and comply with Annex A—ASIO Technical Note 5/12—Compartments within Zone Five areas, and c. before using outsourced ICT facilities operationally obtain ASIO-T4 physical security certification for the outsourced ICT facility to hold information that, if compromised, would have a catastrophic business impact level.

Supporting requirement notes:

Note i The Type 1A security alarm system transition policy details the progressive timeframe for replacement, by 1 August 2021, of the Type 1 Security Alarm System with the Type 1A Security Alarm System in certified and accredited Security Zones Four and Five. Replacement of the Type 1 Security Alarm System with the Type 1A Security Alarm System aims to ensure technology keeps pace with the changing threat environment.

Note ii Unless guard patrols are used instead of a security alarm system in accordance with **Requirement4 aiii**.

Guidance

See Entity facilities at www.protectivesecurity.gov.au

www.protectivesecurity.gov.au

www.protectivesecurity.gov.au