Attachment B—Protective Security Accountable Authority Instruction

Protective Security

a. You must be **familiar** with the agency's security plan, and contribute to a strong and positive security culture within the agency.

b. You must **comply** with protective security policy and procedural requirements, including cyber security policies and procedures and report security incidents or breaches in a timely manner.

s 47F (1)

CEO signature: Date: 21. 12. 2006

AUSTRALIA

Commonwealth of Australia
Acting Chief Executive Officer

Appointment of the Chief Security Officer for the purposes of the *Australian Government Protective Security Policy Framework*

I, AMANDA CATTERMOLE, Acting Chief Executive Officer of Services Australia:

1. APPOINT the person occupying or performing the duties of the position Chief Operating Officer, Corporate Enabling Group, as the Services Australia **Chief Security Officer** as provided for in the Protective Security Policy Framework (PSPF); and

2. AUTHORISE the **Chief Security Officer** to exercise those powers or functions specified in Schedule 1 of this instrument of appointment.

s 47F (1) Dated:. 1 February 2020
s 47F (1)

Amanda Cattermole s 47F (1)
Acting Chief Executive Officer

Schedule 1 Chief Security Officer

Item	
1	Support the Chief Executive Officer as the accountable authority to ensure the safety of people (including staff, contractors, visitors and customers), information and assets.
2	Appoint Security Advisors to provide oversight and management of the agencies security-related functions.
3	Embed efficient and effective security management awareness and practices by setting the strategic direction for protective security planning and risk management.
4	Establish effective procedures to achieve security outcomes that are consistent with the Protective Security Policy Framework (PSPF) and other Australian Government policies and legal requirements.
5	Manage the agency's response to security-related crises, incidents and emergencies in accordance with the agency's security incident and investigation procedures, and establish monitoring mechanisms across the agency.
6	Foster a positive security culture where staff and contractors understand their responsibilities to manage security risk.
7	Ensure information and security awareness training programs are in place so staff and contractors understand their security obligations.
8	Establish security assurance measures to monitor procedures to achieve required protections, address risks, counter unacceptable security risks, and improve security maturity.
9	Oversee the preparation of the agency's PSPF annual security report to accurately reflect the agency's security maturity position and detail how to address areas of vulnerability.

Australian Government
Services Australia

Chief Operating Officer
Russell Egan

Appointment of Security Advisors to support the Chief Security Officer

1. As the Chief Security Officer of Services Australia and for the purposes the Protective Security Policy Framework, I have decided to obtain support in the day-to-day delivery of protective security, and to obtain specialist services from Senior Executive Service officials of Services Australia.

2. I appoint the following officials as **Deputy Chief Security Officers**:
   a. General Manager Corporate and Cross Government Services
   b. General Manager Cyber Security; and
   c. General Manager Fraud Control and Investigations.

3. All **Deputy Chief Security Officers** will provide advice to me and take responsibility for functions and powers specified in Schedule 1 of this appointment.

4. The General Manager, Corporate and Cross Government Services will provide advice to me, and take responsibility for functions and powers specified in Schedule 2 of this appointment.

5. The General Manager, Cyber Security will provide advice to me and take responsibility for functions and powers specified in Schedule 3 of this appointment.

6. The General Manager, Fraud Control and Investigations will provide advice to me and take responsibility for the functions and powers specified in Schedule 4 of this appointment.

s 47F (1)

Russell Egan
Chief Operating Officer (Chief Security Officer)
Services Australia
20 October 2022

Schedule 1

All Deputy Chief Security Officers

Item	Responsibility
1	Support the Chief Executive Officer as the accountable authority, by being responsible for agency-wide oversight of protective security and direct all areas of security to protect the agency's people (including staff/contractors, visitors and customers), information (including ICT) and assets.
2	Appoint security advisors to oversee and manage the agency's protective security-related functions and perform specialist services.
3	Tailor protective security arrangements to the scale and complexity of the agency and its risk environment.
4	Establish effective procedures to achieve security outcomes that are consistent with the Protective Security Policy Framework (PSPF) and other Australian Government policies and legal requirements.
5	Manage the agency's response to security-related crises, incidents and emergencies in accordance with the agency's security incident and investigation procedures, and establish monitoring mechanisms within the agency.
6	Foster a positive security culture where all individuals understand that they are responsible for managing the agency's security risks.
7	Establish security assurance measures to monitor procedures to achieve required protections, address risks, counter unacceptable security risks, and improve security maturity.
8	Assist the Chief Security Officer (CSO) to document any decision to implement an alternative mitigation measure or control to PSPF requirement, and adjust the maturity level for the related PSPF requirement.
9	Contribute to the agency's annual PSPF self-assessment report ensuring it accurately reflects the agency's: • Protective security capability. • Protective security risk environment. • Security maturity against the PSPF self-assessment maturity model. • Strategies and actions to address areas of immaturity or vulnerability.
10	Contribute to the development of a comprehensive security plan to articulate how the agency will manage its security risk, spanning each of the agency's protective security principles.
11	Liaise with law enforcement and intelligence agencies, other emergency services, service providers, clients and stakeholders through agreed arrangements.
12	Disseminate protective security intelligence and threat information to stakeholders within the agency.

Schedule 2

Deputy Chief Security Officer—security advisor for security governance, information security, physical security and personnel security

Item	Power or function
Security Governance	
1	Identify and manage security governance risks.
2	Set the strategic direction for protective security planning and risk management.
3	Coordinate the development and implementation of security plans.
4	Monitor security systems that facilitate the agency's capacity to function, and identify security risk,
5	Provide advice on protective security, and security risk management arrangements.
6	Prepare security governance reports for the CSO or strategic committees, and assist with gathering information to meet annual security reporting obligations.
7	Coordinate and conduct security reviews.
8	Respond to, and coordinate security incident arrangements and be accessible for individuals to discuss security issues or concerns,
9	Promote the agency's security and risk culture, so that individuals value and protect government information and assets.
10	Establish networks and relationships to understand the agency's business functions and vulnerabilities.
11	Ensure security requirements are considered in other agency plans (e.g. business continuity).
12	Ensure protective security training programs are in place so individuals receive relevant information about their security obligations.
13	Oversee preparation and submission of the annual PSPF self-assessment report including: • Liaising with stakeholders. • Compiling the report. • Making arrangements to obtain the accountable authority and CSO's approval. • Providing a copy of the report to the Minister.
14	Report significant security incidents to the relevant external authority in accordance with PSPF reporting requirements.
Information Security	
15	Identify and manage information security risks.
16	Contribute to and assist in the development of information security training programs and activities.
17	Establish procedures for the handling and protective marking of information.
18	Assist to manage appropriate access to information.
19	Safeguard information from information security threats and contribute to awareness of information security obligations, and appropriate use of official information.
20	Provide briefings and advice to individuals on information security matters, including individuals located or travelling overseas.

Item	Power or Function
Personnel Security	
1	Identify and manage personnel security risks.
2	Contribute to and assist in the development of personnel security training programs and activities.
3	Assess and manage the eligibility and suitability of individuals.
4	Assess and manage the ongoing suitability of individuals, and share relevant information where appropriate.
5	Manage the personnel security aftercare program for separation of individuals, including withdrawing access and informing about ongoing security obligations.
6	Provide advice on personnel security, including briefings to individuals located or travelling overseas.
7	Assess and manage requests to waive an uncheckable background or citizenship requirement for security clearance holders on the basis of a risk assessment.
8	Share information of security concern, where appropriate, within the agency, with other agencies and with authorised vetting agencies.
9	Manage the agency's security clearances and security clearance holders.
10	Refer matters of potential fraud or corruption to Business Integrity Division for assessment and potential investigation.
Physical Security	
10	Identify and manage physical security risks.
11	Contribute to, and assist in the development of physical security training programs and activities.
12	Ensure a safe and secure physical environment for the agency's staff, contractors, customers and the public.
13	Ensure a secure physical environment for official resources.
14	Manage physical security measures and access controls to protect facilities, information and physical assets. For example, ensure facilities are certified and accredited in accordance with the PSPF before being used operationally.
15	Liaise with and manage security contractors to deliver security services including: • Security Construction and Equipment Committee (SCEC) endorsed consultants. • Security industry specialists. • Security guards. • Safe hand and overnight couriers. • Secure destruction. • Locksmith services.
16	Undertake strategic planning for preparation of new or green-field sites.

Schedule 3

Deputy Chief Security Officer—Chief Information Security Advisor

Item	Power or Function
Cyber Security	
1	Identify and manage ICT security risks.
2	Ensure appropriate procedures for the secure handling and protective marking of information are established and embedded into the agency's ICT systems.
3	Manage access to information in the agency's ICT systems.
4	Protect the agency's ICT systems against unauthorised access or compromise, and ensure information in electronic form is: • Stored • Processed • Communicated in accordance with the law, Australian Government policies and the agency's cyber security requirements detailed in the agency's cyber security plan.
6	Safeguard information from cyber threats; ensure robust ICT systems.
7	Contribute to awareness of security obligations around appropriate use of ICT equipment and official information.
8	Respond to and manage cyber or ICT security incidents.
9	Provide briefings and advice to individuals on cyber and ICT security, including briefings to individuals located or travelling overseas.
10	Coordinate and conduct ICT security reviews.
11	Liaise with and manage ICT contractors in the delivery of secure services including: • Telephones • Internet and email gateways • Data storage and recovery.
12	Ensure ICT systems are certified and the appropriate level of security is being applied, with residual risks accepted by the relevant accreditation authority.
13	Report significant cyber or ICT security incidents to the relevant external authority in accordance with PSPF reporting requirements.
14	Refer matters of potential fraud or corruption to Business Integrity Division for assessment and potential investigation.

Schedule 4

Deputy Chief Security Officer—General Manager, Fraud Control and Investigations

Item	Power or Function
Investigations	
1	Identify, analyse and where appropriate, undertake a criminal investigation into any irregular or adverse activities or events, threats and behaviours in a timely manner.
2	Assist with the planning, development and delivery of security awareness products and activities.

Australian Government

Services Australia

Protective Security Governance Policy

September 2025

SECURITY BRANCH

Contents

1. Protective Security Governance Policy

1.1 Overview

1.1.1 The Protective Security Governance Policy (the Policy) sets out how Services Australia (the agency) complies with the mandatory security governance requirements of the Australian Government Protective Security Policy Framework (PSPF).

1.1.2 The PSPF assists Australian Government entities to protect their people, information and resources, both domestically and internationally.

1.1.3 The PSPF articulates the Government's protective security policy. It guides entities on effective implementation across security domains, governance, risk, information, technology, personnel and physical.

1.1.4 The agency must manage security risks and support a positive security culture. The agency must ensure accountabilities are clear and has in place sound planning, investigation and response, assurance, review processes, and accurate reporting.

1.1.5 This governance policy comprises six subordinate security governance sections:

- Establish responsibilities for protective security and governance arrangements.
- Develop a Security Plan.
- Embed security culture and security awareness.
- Detect and respond to security incidents.
- Assess and report on our security capability.
- Review and improve to security uplift.

1.1.6 The Policy applies to all agency staff, including ongoing and non-ongoing staff, labour hire, consultants and third-party providers.

1.1.7 Where the Policy uses the term "security", this refers to protective security.

1.1.8 This Policy is specific to the security governance domain. Separate Policy statements apply to the information, personnel and physical security domains.

1.2 More information

1.2.1 For more information regarding this policy, email s 47E (d)

1.2.2 For definitions of security terms refer to the Security Hub.

2. Role of the Accountable Authority

2.1.1 The Accountable Authority for protective security in Services Australia is the Chief Executive Officer.

2.1.2 Under the Public Governance, Performance and Accountability Act 2013, the Accountable Authority must establish appropriate systems of risk oversight and management for the entity, including the implementation of the PSPF to protect the agency's people, information and resources.

2.1.3 The Accountable Authority must:

- appoint a Chief Security Officer (CSO) at the SES Band 1 level or above
- appoint a Chief Information Security Officer (CISO), responsible for the cyber security program and the cyber security of the agency's most critical technology resources
- determine the agency's tolerance for security risk, balancing the agency's requirements to deliver business objectives and maintain a secure environment
- manage the security risks of the agency effectively, including identifying, assessing and prioritising risks to people, information and resources
- actively consider the implications that risk management decisions may have for other government entities, and share information on risks where appropriate
- determine any decision to vary the agency's application of a PSPF requirement to assist the

agency manage exceptional circumstances for a temporary period
- ensure decisions to vary the agency's application of a PSPF requirement are recorded in the annual protective security report.

2.1.4 The agency's approach to satisfy these mandatory responsibilities is set out in the **Protective Security Plan 2023-25**.

3 Management structures and responsibilities

3.1 Overview

3.1.1 The CSO supports the Accountable Authority to deliver the agency's security outcomes by providing strategic, agency-wide oversight of security across security governance, information security, personnel security and physical security.

3.1.2 The CSO appoints **Security Practitioners** to perform security functions or specialist services to support the CSO and CISO in the day to day functions of protective security.

3.1.3 The CISO supports the Accountable Authority and complements the CSO role to ensure a holistic approach to security is maintained.

3.1.4 The Protective Security Plan 2023-25 states the powers and functions of the CSO and the agency's Security Practitioners.

3.2 Security Committee

3.2.1 The PSPF requires the CSO to achieve and maintain the required level of protective security oversight and accountability across all areas of security for the agency.

3.2.2 The agency has established the Security Committee to ensure effective oversight of protective security capabilities across the agency. The Security Committee supports the Accountable Authority and CSO by:

- approving security plans and frameworks that strengthen the 6 Protective Security Policy Framework (PSPF) domains: governance, risk, information, technology, personnel and physical
- endorsing enterprise security strategies for EC's decision
- advising EC and individual accountable officers on security threats, potential implications and mitigation strategies
- advising EC and individual accountable officers on priority systemic incidents, investigations and audits
- providing advice on plans and initiatives across the PSPF domains
- monitoring emerging and evolving risks and threats across the security landscape
- overseeing the implementation of government security policy requirements within the PSPF, Information Security Manual and the Essential 8 cyber mitigation strategies
- oversight of the Cyber Work Program and the Insider Threat Program
- monitoring progress to implement recommendations arising from high priority investigations, audit and security reviews such as the Ashton Review
- overseeing planning and controls to mitigate security threats and adverse events
- ensuring effective investment in staff awareness and adherence to a positive security

3.3 Security policy and procedures

3.3.1 The Accountable Authority, supported by the CSO, is responsible for ensuring the agency has put in place security policies and procedures that inform staff on practices that reflect the agency's implementation of PSPF requirements. The Security Branch will regularly review these policies and procedures to ensure accuracy of the contents.

3.3.2 Agency security procedures are accessible from the agency's Security Hub.

3.3.3 The PSPF requires entities to maintain and monitor an email address as a central point of contact and conduit for all security matter across governance, personnel, information, physical security, risk and technology. The agency's email address is s 47E (d)

3.4 Protective Security Plan 2023-25

3.4.1 Agencies **must** have a security plan approved by the Accountable Authority, to manage the agency's security risks.

3.4.2 The agency's Protective Security Plan 2023-25 addresses all PSPF mandatory elements required of a security plan, This includes:

- agency's security goals and strategic objectives
- agency's operating environment, threats, risk and vulnerabilities that impact the protection of our people, information and resources
- detailing the agency's tolerance and capacity to manage security risks
- detailing the agency's mitigation strategies
- sharing of risk management decisions that may impact other entities
- detailing how the agency will implement the requirements of the PSPF
- detailing the agency's arrangements for implementing any direction issued by the Secretary of the Department of Home Affairs under the PSPF
- identification of critical personnel and resources to ongoing operations of the agency
- agency's security threat levels which scaled against the agency' operational environment and the national threat environment
- agency's security incident management plan
- agency's monitoring and improvement arrangements
- agency's mechanism to review the plan and respond to any significant shifts in the security environment.

3.4.3 In accordance with PSPF requirements the security plan must be reviewed at least every two years.

3.4.4 The Protective Security Plan 2023-25 is accessible from the agency's Security Hub.

3.5 Agency Security Threat Assessment

3.5.1 The agency has an Agency Security Threat Assessment (ASTA) which provides an enterprise-level assessment of the current security environment in which we operate.

3.5.2 The ASTA details the threat rating levels against the identified malicious actors who have been assessed as having both the intent and capability to carry out an attack against the agency. It also provides an overview of the appropriate classification level of that intent and capability and how it could be used against us.

3.6 Impacts of risks

3.6.1 Agencies **must** communicate to the affected Commonwealth entity any identified risk that potentially impacts that entity.

3.6.2 Communicating with affected entities facilitates the affected entity's response and enables entities to cooperate to manage shared risks.

3.6.3 For information on the agency's approach to managing risk including those shared risks with other entities, refer to the agency's Networks and Partnerships Team.

4 Security Culture and Awareness

4.1 Security culture

4.1.1 It is the responsibility of the Accountable Authority and the CSO, to develop, implement and maintaining a program to foster a positive security culture and provide staff sufficient security information and training.

4.1.2 A strong and healthy security culture helps to safeguard the agency's staff, information and resources, engenders trust, encourages consistent positive security behaviour and supports staff to engage proactively with risk.

4.1.3 Within the agency, the Services Australia Protective Security Plan 2023-25 clarifies how the Accountable Authority, CSO, CISO and senior leadership prioritise and promote security across the agency. This includes ensuring:

- security is built into the agency's business operations and decision making
- security is seen as a business enabler, supporting accessibility of services
- security risks are proactively identified and treated, and staff understand those risks and their responsibilities in relation to them
- security incidents and breaches are reported, recorded and investigated appropriately according to clear agency procedures
- implementation of security policies is mature and well-managed
- security procedures are easy to understand, current and accessible
- classified information is protected from unauthorised disclosure or compromise and personnel apply the need-to-know principles
- security improvements are encouraged and promoted

4.2 Security awareness training

4.2.1 Security awareness training is an important element of security and supports the implementation of physical, information and personnel security policies, practices and procedures.

4.2.2 The agency provides security awareness training to all staff upon commencement and annually thereafter to ensure they understand their obligations and responsibilities, including

- awareness that security is everyone's responsibility
- able to understand and comply with security-related obligations and agency practices and procedures
- equipped and supported to engage with risk and make risk-based decisions
- aware of the consequences of non-compliance with security practices and procedures
- confident in making decisions on applying protective markings, storing and sharing government information

4.2.3 The agency provides specific security training to specialists and staff occupying designated high-risk positions.

4.2.4 For further information refer to Security resources and training.

4.3 Security Incidents

4.3.1 The agency must report any significant or reportable security incidents to the relevant authority.

4.3.2 The CSO, with support from the CISO for cyber security incidents, is responsible for establishing a security incident management plan, and incorporating into the agency's business continuity arrangements to ensure that business-critical people, operations, systems and services are supported appropriately in the event of an incident or disaster.

4.3.3 The CSO is responsible for investigating, responding to and reporting on security, the CISO is responsible for investigating, responding to and reporting on cyber security incidents.

4.3.4 The agency has developed procedures to ensure security incidents are responded to and, where required appropriately investigated.

4.4 Policy changes due to exceptional circumstances

4.4.1 Agencies **must** document any deviation from PSPF requirements or decision to approve an alternative approach to implement a PSPF requirement.

4.4.2 Decisions to deviate from PSPF requirements due to exceptional circumstances **must** be notified to s47E(d)

4.4.3 Decisions to vary the application of a PSPF requirement are recorded in the annual PSPF security maturity report.

5 Protective Security Reporting

5.1.1 Agencies must provide an annual protective security report (the report) to the Department of Home Affairs and to the agency's Minister, reporting on the compliance with:

- their security obligations
- implementing sound and responsible protective security practices
- identifying and mitigating security risk and vulnerabilities

5.1.2 The agency reports its compliance of each PSPF requirement across the six domains.

5.1.3 There are three reporting categories for each PSPF mandatory requirement:

- fully implemented
- risk managed, or
- not yet implemented

5.1.4 The CEO as Accountable Authority approves the report and the CSO submits the report to the Department of Home Affairs.

5.1.5 For further information on security reporting, email s47E(d)

6 Document control

Version	Date	Author(s)/Reviewer(s)	Comments
1.0	September 2020	s 47F (1)	First version
1.1	February 2021	s 47F (1)	Minor updates to text. Links to Protective Security Control Plan 2020- 22. Updates to links to existing documents. Reference to new Protective Security AAI
1.2	August 2022	s 47F (1)	Updated links to existing documents
1.3	November 2022	s 47F (1)	Update to links. Updates to text to reflect changes to the PSPF. Update to text to reflect the change of document names.
1.4	January 2023	s 47F (1)	Update to links
1.5	August 2023	s 47F (1)	Updated text to reflect change of document name and links to PSP

			2023-25
1.6	September 2023	s 47F (1)	Update to 3.4.1 to include review of policies of procedures.
1.7	October 2023	s 47F (1)	Update to 3.4.1 to include review of policies of procedures.
1.8	December 2023	s 47F (1)	Review of content to align with PSPF Policy 2 changes and minor updates, including corporate branding
1.9	September 2025	s 47F (1)	Review and update of content to align with PSPF Release 2025

7 Document endorsement

Status	Approved
Issue Date	March 2024
Issuing Authority	s 47F (1) , Director, Security Branch

servicesaustralia.gov.au

Australian Government

Services Australia

Information Security Policy

SECURITY BRANCH

Contents

1. Information Security Policy

1.1. Overview

1.1.1. The Information Security Policy (the Policy) sets out how Services Australia (the agency) complies with the mandatory information security requirements of the Australian Government Protective Security Policy Framework (PSPF).

1.1.2. For this Policy, information is defined as physical documents/papers, electronic/digital data, verbal communications or intellectual information (knowledge) that is collected, created, used, managed or maintained by the agency.

1.1.3. The PSPF assists Australian Government entities to protect their people, information and resources, in Australia and overseas. The PSPF articulates the Government's protective security policy. It also guides entities on effective implementation of the policy across six security domains: governance, risk, information, technology, personnel and physical.

1.1.4. The four PSPF Release 2025 sections under the Information Domain are:

- PSPF Section 9 : Classifications and Caveats
- PSPF Section 10 : Information Holdings
- PSPF Section 11: Information Disposal
- PSPF Section 12 : Information Sharing

1.1.5. This Policy applies to all agency staff. Where the term 'staff' is used, this relates to all employees and contractors.

1.1.6. Where this Policy uses the term ‘security,’ this refers to protective security.

1.1.7. This Policy is specific to information security. Separate policy statements apply to physical, governance and personnel security.

1.2. More information

1.2.1. A list of security definitions can be found on the intranet.

1.2.2. For more information regarding this Policy, email s 47E (d)

2. Official and security classified information

2.1. Overview

2.1.1. This Policy details the agency's obligations for official and security classified information, and the handling arrangements required to protect this information.

2.1.2. Information is a valuable resource and protecting the confidentiality, integrity and availability is vital to business operations including access provided in contracts for goods and services. This includes various forms of information such as physical documents and electronic devices.

2.1.3. The agency must:

- identify all information holdings and assess the sensitivity and security classification of information
- implement control measures to protect this information adequately
- ensure all information is accessed, handled, stored and transmitted appropriately.

2.2. Identifying and assessing the security classification of information

2.2.1. The originator of information must determine the appropriate security marking. All information created, sent or received as part of the work of the agency and Australian Government is official information and a record, and it provides evidence of what the agency has done and why. All official information requires an appropriate level of protection. Security classified information requires stronger protection to prevent damage to the national interest that may arise through loss or compromise of that information.

2.2.2. If the originator of information is unavailable, staff inheriting the originator's business role responsibilities or functions will become the originator. If the business ownership of the information cannot be determined, for example when a business area no longer exists, contact s47E(d) or assistance.

2.2.3. All security classified information must have the appropriate protective security classification or markings applied (for example, OFFICIAL: Sensitive). The security markings identify what level of information protection and access control requirements apply.

2.2.4. For information classified PROTECTED and above additional security caveats may be applied where information has special protections and handling requirements in addition to those indicated by the security classification.2.2.5. Originators must determine and set the protective security marking at the lowest reasonable level for that piece of information, balancing the need to protect information without unnecessarily hindering business operations.

2.2.5. Originators can reclassify information when it is appropriate at any point in time. This can include establishing a process for reclassification including an automated process. The conditions for automatic reclassification must be established and documented in the information. Security markings on documentation must be adjusted when reclassifying.

2.2.6. The appropriate security marking is determined using a type of risk rating system called 'Business Impact Levels' (BIL) as summarised briefly described in Table 1 below.

2.2.7. For further information, refer to Security Markings.

Table 1. Protective markings and Business Impact Levels

Protective marking	Business Impact Level (BIL)	Damage if information is compromised
OFFICIAL	LOW business impact	No or negligible damage. This accounts for the majority of routine business information. This includes personal information not defined as sensitive under the *Privacy Act 1988.*
OFFICIAL: Sensitive	LOW to MEDIUM business impact	May result in limited damage to an individual, organisation or government of compromised. This includes personal information as defined sensitive under the *Privacy Act 1988,* information about the agency's capability, assets and finances, legal compliance, security control frameworks or an individual's criminal record etc.
PROTECTED	HIGH business impact	Would be expected to cause damage to the national interest, organisations or individuals. This includes information that would be expected to result in the agency not being able to perform one or more of its primary functions, or a significant aggregation of sensitive data.
SECRET	EXTREME business impact	Would be expected to cause serious damage to the national interest, organisations or individuals.
TOP SECRET	CATASTROPHIC business impact	Would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.

2.2.8. For further information, refer to Business Impact Levels.

2.3. Implementing control measures to protect information

2.3.1. The agency must manage information appropriately including:

- correctly marking all security classified information
- reclassifying or sanitising security classified information when appropriate
- providing access to all security classified information only to those with a need to know
- using and discussing classified information only in appropriate facilities
- storing all security classified information in appropriate containers
- carrying and transferring security classified information in accordance with appropriate processes
- securely disposing of security classified information
- correctly handling digital devices.

2.3.2. For further information, refer to the Information Security and the Cyber Security Policies intranet pages.

2.3.3. Staff must adhere to the agency's clear desk or end of day security processes to protect information and information assets (ICT equipment, portable storage devices and security cabinet keys) when not in use.

2.3.4. For further information refer to:

- Clear Desk

- Security Markings
- Information handling guide
- Cyber Central
- Asset Disposal Procedures
- Privacy Policies
- Working Away from the Office
- Secure storage of information
- Transporting Documents

3. Access to information

3.1. Overview

3.1.1. The agency must put in place appropriate security controls to protect its official information (including higher classifications of information) balancing the need to maintain the provision of timely, reliable and appropriate access to official information to support business outcomes.

3.1.2. It may be an offence under the *Crimes Act 1914* or the *Criminal Code* to share or disclose information inappropriately. In addition, it is necessary to limit sharing of information depending on the purpose it was collected. Secrecy provisions apply to various legislation underpinning social security, family assistance and other health and welfare programs.

3.2. Sharing information

3.2.1. The agency must ensure access to official information, including security classified information, is only provided to individuals where there is a "legitimate need to know."

3.2.2. When sharing official information with non-government entities the agency must have a written agreement, such as a contract, deed or Memorandum of Understanding, that require relevant parties to the agreement, to appropriately protect security classified information.

3.2.3. Agreements must include requirements for notifying the agency if information is lost or compromised and that the supplier will not act or engage in a practice that would breach the *Privacy Act 1988* or the *Australian Privacy Principles*.

3.2.4. The agency should regularly monitor to ensure such agreements exist, are current, are valid and are an effective control.

3.2.5. An individual must possess the appropriate security clearance to access security classified information. For further information, refer to Security Clearances.

3.3. Ensuring a legitimate 'need-to-know' exists

3.3.1. The need to know" must not be based on convenience, position, level, or assumed privilege.

3.3.2. Staff have a genuine 'need-to-know' if they meet the following three requirements:

- without access, they would be hindered in the proper or efficient performance of their duties
- their 'need-to-know' is authorised by their business area

- they have the appropriate level of security clearance to access the information provided, and the level of security clearance is current and confirmed.

Table 2. Access requirements for sensitive and security classified information

Information type	Protective marking	Access requirements	Security zone requirements
Non business information	UNOFFICIAL	No requirements	All areas including public access areas
Business information – information created, sent or received as part of the work of government	OFFICIAL	Access restricted to individuals with a genuine need to know	All areas including public access areas
Sensitive information - business related that is private or confidential or valuable	OFFICIAL: Sensitive	Access restricted to individuals with a genuine need to know, including agency staff or contracted individuals	Non-public access areas of the agency
Information that would be expected to damage individuals, organisations or the national interest if compromised	PROTECTED	Access restricted to individuals with a genuine need to know, including agency staff or contracted individuals Baseline security clearance	Non-public access areas of the agency
	SECRET	Access restricted to individuals with a genuine need to know, including agency staff or contracted individuals Negative Vetting Level 1 security clearance	Agency non-public areas with limited staff and contractor access. Minimum Zone 3 but preferably Zone 4*
	TOP SECRET	Access restricted to individuals with a genuine need to know, including agency staff or contracted individuals Negative Vetting Level 2 security clearance	Agency non-public areas with limited staff and contractor access and strong access protections. Minimum Zone 4 but preferably Zone 5**

* Must meet Zone 3 specifications as prescribed by the PSPF. For further information refer to the Security of our sites intranet page or contact s47E(d) to clarify the Zone of your work area.

** Must meet Zone 4 specifications as prescribed by the PSPF. For further information refer to the Security of our sites intranet page or contact s47E(d) to clarify the Zone of your work area.

4. Document control

Version	Date	Author(s)/Reviewer(s)	Comments
1.0	September 2020	XX	XX
1.1	February 2021	s 47F (1)	Review of content and fixing links to existing procedures
1.2	December 2022	s 47F (1)	Review of content and added links to Privacy and Records Management
1.3	March 2023	s 47F (1)	Review and update to reflect: • additional information regarding classification and reclassification • PSPF Policy 8 changes
1.4	November 2023	s 47F (1)	Review and update to reflect: • PSPF Policy 8 changes • Corporate branding updates
1.5	September 2025	s 47F (1)	Review and update to reflect PSPF Release 2025 changes

5. Document endorsement

Status	Approved
Issue Date	2023
Issuing authority	s 47F (1) , Acting Director, Security Branch

servicesaustralia.gov.au

Australian Government

Services Australia

Physical Security Policy

V1.2

July 2025

OFFICIAL

Corporate and Cross Government Services Division | Security Branch

Contents

Purpose

This policy describes the physical security protections required for Services Australia (the agency) to minimise or remove security risk to safeguard its people, information and resources in accordance with the requirements of the Protective Security Policy Framework (PSPF). Through the implementation of this policy, the agency provides a secure physical environment for its people, information and resources.

To achieve ongoing and effective delivery of Australian Government business, entities are required to comply with the mandatory requirements of the six (6) domains of the PSPF—governance, risk, information, technology, personnel and physical. The agency Protective Security Control Plan (the plan) 2024-25 outlines how the agency will further strengthen its capability to address current and emerging protective security threats, and more strongly embed security into the agency business and culture. The plan outlines how the six security outcomes combine to ensure security risks are holistically managed.

This policy covers the physical security outcome and its core and supporting requirements. Separate policies apply to security governance, personnel security and information security. This policy should be read in conjunction with supporting physical security procedural documents.

This policy applies to all agency staff, including contractors. Where the term 'staff' is used, this refers to all ongoing and non-ongoing staff, labor hire (contractors), consultants, third party providers and other government department or agency personnel with access to agency people, information and assets.

The term 'must' is used in this policy in accordance with the requirements defined in the PSPF.

Policy overview

The PSPF sets out the requirements for protective security to ensure the secure and continuous delivery of government business. It details the mandatory core and supporting requirements for protective security and provides guidance to support effective implementation of those requirements. The PSPF is applied through a risk management approach, with a focus on fostering a positive culture of security.

Physical security core requirements

The PSPF protective security outcome for physical security is the *"the protection of Australian Government people, information and physical resources secured by those facilities."*

The PSPF core requirements for physical security are detailed as follows:

Requirement:	Details:
189	Protective security is integrated in the process of planning, selecting, designing and modifying entity facilities for the protection of people, information and resources.
190	A facility security plan is developed for new facilities, facilities under construction or major refurbishments of existing facilities.
191	Decisions on entity facility locations are informed by considering the site selection factors for Australian Government facilities.
192	When designing or modifying facilities, the entity secures and controls access to facilities to meet the highest risk level to entity resources in accordance with Security Zone restricted access definitions.

193	Facilities are constructed in accordance with the applicable ASIO Technical Notes to protect against the highest risk level in accordance with the entity security risk assessment in areas: • accessed by the public and authorised personnel, and • where physical resources and technical assets, other than security classified resources and technology, are stored.
194	Facilities for Security Zones Two to Five that process, store or communicate security classified information and resources are constructed in accordance with the applicable sections of ASIO Technical Note 1/15 – Physical Security Zones, and ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas.
195	Entity facilities are operated and maintained in accordance with Security Zones and Physical Security Measures and Controls.
196	Security Zones One to Four are certified by the Certification Authority in accordance with the PSPF and applicable ASIO Technical Notes before they are used operationally.
197	Security Zone Five areas that contain TOP SECRET security classified information or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level, are certified by ASIO-T4 before they are used operationally.
198	Security Zones One to Five are accredited by the Accreditation Authority before they are used operationally, on the basis that the required security controls are certified and the entity determines and accepts the residual risks.
199	Sensitive Compartmented Information Facility areas used to secure and access TOP SECRET systems and security classified compartmented information are accredited by the Australian Signals Directorate before they are used operationally.
200	Physical security measures are implemented to minimise or remove the risk of information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
201	Physical security measures are implemented to protect entity resources, commensurate with the assessed business impact level of their compromise, loss or damage.
202	Physical security measures are implemented to minimise or remove the risk of harm to people.
203	The appropriate container, safe, vault, cabinet, secure room or strong rooms is used to protect entity information and resources based on the applicable Security Zone and business impact level of the compromise, loss or damage to information or physical resources.
204	Perimeter doors and hardware in areas that process, store communicate security classified information or resources are constructed and secured in accordance with the physical security measures and controls for perimeter doors and hardware.
205	Access by authorised personnel, vehicles and equipment to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for authorised personnel.
206	Access by visitors to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for visitors.

207	The Accountable Authority or Chief Security Officer approves 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, on the basis that the person: • has the required security clearance level for the Security Zone/s, and • a business need supported by a business case and security risk assessment, which is reassessed at least every two years.
208	Unauthorised access to Security Zones One to Five is controlled in accordance with the physical security measures and controls for security alarm systems.
209	Security guard arrangements in Security Zones One to Five are established in accordance with the physical security measures and controls for security guards.
210	Technical surveillance countermeasures for Security Zones One to Five are established in accordance with the physical security measures and controls for technical surveillance countermeasures.

Physical security principles

The agency uses a risk-based approach to physical security at its sites to mitigate identified and emerging security risks, aligned with the agency's priorities and objectives. The agency uses security-in-depth, incorporating a multi-layered security design to protect the agency's people, information and resources.

Layering physical security measures means the protection of the agency's people, information and resources are not significantly reduced with the loss or breach of any single layer.

The agency's physical security measures incorporate the following physical security principles:

- **Deter** – measures implemented that adversaries perceive as too difficult, or needing special tools and training to defeat (e.g. access control, security containers)
- **Detect** – measures implemented to determine if an unauthorised action is occurring or has occurred (e.g. CCTV, alarm systems)
- **Delay** – measures implemented to impede an adversary during an attack, or slow the progress of a detrimental event to allow a response before Agency information or physical resources are compromised (e.g. construction of sites)
- **Respond** – measures taken once an agency is aware of an attack or event to prevent, resist or mitigate the attack or event (e.g. security incident response)
- **Recover** – measures taken to restore operations to normal (as possible) following an incident (e.g. business continuity procedures, training and awareness).

Security Construction and Equipment Committee (SCEC) evaluates security equipment for suitability of use by the Australian Government. The PSPF mandates circumstances when the agency must use SCEC-approved equipment to protect its resources and facilities.

The agency may use SCEC-approved security equipment even where it is not mandated. The agency's Physical Security Technical Notes and design guidelines outline when SCEC-approved equipment must be used and when approved commercial equipment can be used.

Risk mitigation and assurance measures

Overall accountability for security risk management rests with the Accountable Authority and as such the agency undertakes physical security mitigation measures to safeguard its people, information and resources from identified risks through a security risk management process.

The key elements of the security risk management process are:

- **Security risk assessment** – A structured and comprehensive process to identify, analyse and evaluate security risks and determine practical steps to minimise those risks.
- **Security risk treatment** – A considered, coordinated and efficient actions and resources required to mitigate or lessen the likelihood of negative consequences of risk.

The agency therefore undertakes security risk assessments in line with the relevant standards to protect resources commensurate with the assessed business impact level of their compromise, loss or damage, including:

- minimising or removing the risk of harm to people,
- minimising or removing the risk of information or resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorization,
- selecting appropriate containers, cabinets and secure rooms to protect information and resources and
- Disposing of physical assets securely

Physical security for entity resources

Identifying entity resources

Resources refers to people, information and resources that the agency uses in its operations, including third party provider sites or in use by co-location partners in agency sites. This includes, but is not limited to, people, information, office tenancies, furniture, electronic assets as well as other resources that enable the agency to conduct business.

The agency provides and maintains an appropriate physical security environment to protect its people and people attending its sites. This physical security environment is also required to protect official information and resources secured at those sites.

People

The *Work Health and Safety Act 2011* provides the framework to safeguard the health and safety of workers and workplaces. The PSPF requires entities to implement appropriate physical security measures to ensure the personal security of its people while working in the office and working away from the office in compliance with the *Work Health and Safety Act 2011*.

Refer to the agency's HR Policy Hub for details on work health and safety requirements.

Information

Information is a valuable resource and requires protection in accordance with the sensitivity of the information to ensure confidentiality, integrity and availability of information. PSPF requires entities to correctly assess the sensitivity or security classification of information and adopt marking, handling, storage and disposal arrangements that guard against information compromise. It is also essential that information is readily available to support efficient business operations.

Refer to the agency's Information Security Policy for details on information security requirements.

Resources

Physical assets are tangible items that are valuable to the agency and require protection. The level of protection for different physical assets will be determined by the category of assets and the business level impact of the compromise, loss or damage of the asset. Asset control assists with the identification of assets and their protection from theft, damage and loss. The PSPF recommends entities implement appropriate asset control for identified physical assets.

Refer to the agency's Asset Management Policy for details on the requirements for accounting, controlling and monitoring all tangible non-financial assets.

Refer to the agency's Cyber Security Policies for details on ICT equipment requirements.

Physical security measures to protect entity resources

The PSPF requires the agency to implement appropriate physical security measures to minimise the risk of resources being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation.

The agency enhances physical security measures by using security in layers via combinations of procedural and physical security measures, including but not limited to:

- security zones
- security containers and cabinets
- identity and building access cards.

Business Level Impact Assessment

The agency must put in place physical security measures to protect its resources, commensurate with the assessed business impact level of their compromise, loss or damage and implement appropriate security measures required to achieve effective protection.

The PSPF defines the level of damage or impact on business operations that could result from a compromise, loss or damage of physical assets as provided in Table 1.

Table 1 Business Impact Levels—compromise, loss or damage of physical assets

1 – Low business impact	**2 – Low to medium business impact**	**3 – High business impact**	**4 – Extreme business impact**	**5 – Catastrophic business impact**
Compromise, loss or damage of assets could be expected to cause **insignificant damage** to an individual, organisation or government.	Compromise, loss or damage of assets could be expected to cause **limited damage** to an individual, organisation or government.	Loss or damage of assets would be expected to cause **damage** to the national interest, organisations or individuals.	Compromise, loss or damage of assets would be expected to cause **serious damage** to the national interest, organisations or individuals.	Compromise, loss or damage of assets would be expected to cause **exceptionally grave damage** to the national interest, organisations or individuals.

***Refer** to the agency's Business Level Impact Assessment procedure for further information.*

***Refer** to the agency's Information Security Policy for the business impact levels relating to the compromise of the confidentiality of information.*

Security Zones

Security zones provide a methodology for scalable physical security risk mitigation applied based on the agency's security risk assessment. The agency designs and modifies its sites according to the five security zones, with security measures increasing for each level up to Zone Five.

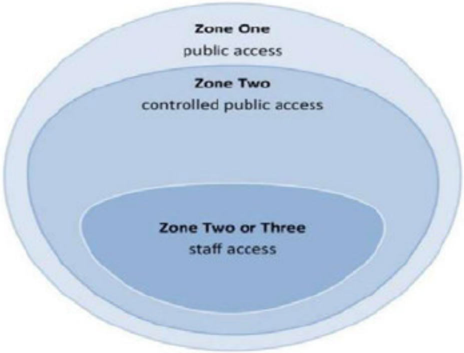
The PSPF defines five levels of security zones as provided in Table 2.

Table 2: Defined security zones

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 is 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 is 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 is 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

To support the security-in-depth principle, the agency's security zones may be layered where there is a need to provide greater protection to personnel and restrict access to information and assets.

Figure 1: Example of layering security zones



Security containers, cabinets and rooms

The agency must assess security risks and select the appropriate secure room, container or cabinet to store and protect sensitive and security classified information and assets.

Refer to the agency's Information Security Policy for further details on information security requirements.

Security containers and cabinets

The agency uses SCEC-approved security containers and cabinets for the protection of security classified information and assets.

There are three levels of SCEC-approved containers:

- Class A: Protects information that has an extreme or catastrophic business impact level in situations assessed as high risk.
- Class B: Protects information that has an extreme or catastrophic business impact level in situations assessed as low risk, or for information that has a high or extreme business impact level in situations assessed as higher risk.
- Class C: Protects information up to an extreme business impact level in situations assessed as low risk, or for information that has a medium business impact level in situations assessed as higher risk.

Table 3 details the storage container requirements for the storage of information and assets based on the security zone of the area where the secure container is located.

Table 3: Security zone storage container requirements (Zone One to Zone Three) *

	Zone One	Zone Two	Zone Three
UNCLASSIFIED (including DLM)	Commercial Grade	Commercial Grade	Commercial Grade
PROTECTED	Not Permitted	SCEC Class C	SCEC Class C
SECRET	Not Permitted	Not Permitted	SCEC Class B

***** Contact the Physical Security Infrastructure Team for details of Zone Four and Zone Five requirements.***

Keys to security containers and cabinets should be secured in key cabinets within the agency's secure perimeter and where possible within the security zone where the containers and cabinets are located. For security containers and cabinets that are secured using combination settings, the combination settings should be changed every six months (minimum), and/or following repairs change of staff or where it is suspected that the combination may have been compromised.

Secure rooms

Secure rooms may be used instead of secure containers and cabinets to secure large quantities of official information, classified assets and valuable assets, where the compromise, loss or damage would have a business level impact. Prior to any proposal for the design or modification of a secure room, the Physical Security Infrastructure Team must be consulted

Security requirements for disposal of physical assets

The agency must dispose of physical assets securely. Disposal of assets covers the sale, destruction, scrapping, transfer or gifting of physical assets.

Prior to decommissioning and disposing of physical assets (such as security containers and cabinets, commercial safes and vaults, and secure rooms), staff must:

- reset combination locks (electronic and mechanical) to factory settings
- visually inspect and remove all contents from these physical assets.

Refer to the agency's Disposal of Services Australia assets procedure for further details on the requirements for the disposal of assets.

Physical security for entity facilities

The agency must ensure it fully integrates protective security in the process of planning, selecting, leasing/purchasing, designing and modifying its facilities for the protection of people, information and physical assets.

Planning and site selection

The agency's site location selection process incorporates a physical security site inspection and assessment. The assessment includes consideration of the suitability of the physical security environment of a proposed site for entity facilities and the security measures that need to be constructed or modified to provide appropriate risk mitigation strategies whilst accommodating normal business. This may include use of Crime Prevention through Environmental Design.

The agency's Physical Security Infrastructure Team must be consulted prior to any proposal for the planning or selection of agency facilities.

Site security plans

All sites where the agency's resources are located on an ongoing basis must have a site security plan. A site security plan documents measures to mitigate identified risks to the agency's functions and resources at the site. The form of site security plans will differ depending on the site's asset class (i.e. customer facing site, office, etc.).

Designing and modifying facilities

The protection of people, information and assets is achieved through a combination of physical and procedural security measures that prevent or mitigate threats and attacks.

When designing or modifying its facilities, the agency must consider protective security measures as part of the site due diligence process. The PSPF mandates that the agency designs and modifies its facilities to secure and control access that meets the highest identified risk levels to the agency's resources.

The agency's Physical Security Infrastructure Team must be consulted prior to any proposal for the design or modification of agency facilities.

Building construction

Security zones must be constructed to protect against the highest identified risk level in accordance with the agency's security risk assessment where information and physical assets, including sensitive and security classified assets are stored. The agency applies security controls for each zone consistent with PSPF requirements.

The agency must construct Zone One to Zone Five areas in accordance with the PSPF requirements, relevant ASIO Technical Notes, and the agency's Physical Security Technical Notes and design guidelines.

The agency's Physical Security Technical Notes and design guidelines detail the minimum standards for construction methods and security devices approved for use in agency sites. The specifications must be used in conjunction with a site security risk assessment to ensure the controls adequately mitigate the identified risks. Where the controls are insufficient to reasonably mitigate the identified risks, additional controls must be implemented through the construction phase.

Physical security measures to protect agency facilities

Identity and building access cards (security pass).

Physical access to the agency's facilities must be authorised. Identity and building access cards identify personnel and ensure only those who are authorised have appropriate access to agency facilities. The agency uses identity and building access cards in all its facilities, regardless of the security zone.

An identity and building access card will be issued to a staff member or contractor following satisfactory completion of a Pre-Engagement Check. An identity and building access card must be properly displayed at all times while at agency facilities, and must not be shared, left unsecured or altered in any way. Staff and contractor access to agency facilities is limited to those areas required for the proper or efficient performance of their duties and their level of pre-engagement check or security clearance.

A visitor is anyone who is not authorised through the pre-engagement check process to have unescorted access to all or part of an agency facility or facilities. Visitors must record their details in a visitor register, be issued with a visitor pass and be escorted at all times when in a non-public area of an agency facility.

Where a person behaves unacceptably on the agency's sites they should be directed to cease their behavior and/or leave the site. Police officers and staff with delegation under the *Public Order (Protection of Person and Property) Act 1971* are able to direct people to vacate the premises if required. If a person refuses to leave, the police should be called. Staff should not attempt to physically remove a person from the agency's facilities.

Refer to the agency's Personnel Security Policy for further information.

Electronic access control and security alarm systems

The agency uses electronic access control in conjunction with security alarms at its facilities to restrict unauthorised access. There are limited areas within agency facilities that may be accessed without control during specified times (usually business hours). These areas generally include public foyers, and customer service areas where there is no segregation of authorised personnel from the public.

The agency undertakes regular access control system audits to confirm whether personnel have a continued need for access.

The agency must use either a Class 5 (AS/NZS 2201.1) or SCEC approved Type 1A security alarm system for Zone Three areas, in addition to a high security access control platform (as specified in the Physical Security Technical Notes). Ongoing access to Zone Three areas must be restricted to people with appropriate security clearance. The agency maintains a record of authorised access and regular audits and reviews activity in Zone Three areas.

Prior to any proposal for the construction of a Zone Three area, the Physical Security Infrastructure team must be consulted.

The agency must use a SCEC-approved Type 1A security alarm system for Zone Four or above, which must be designed, tested and commissioned in accordance with the advice provided by a SCEC-endorsed Security Zone consultant. Prior to any proposal for the construction of Zone Four to Zone five areas, the Physical Security Infrastructure Team must be consulted.

The agency must use dual authentication for access control to Zone Five areas. Dual authentication requires the use of factors from two different security categories (e.g. an identification and building access card in conjunction with a personal identification number). The agency may use dual authentication where not mandated where a risk assessment identifies a need to mitigate the risk of unauthorised access, or otherwise specified in its Physical Security Technical Notes.

Duress alarms

The agency uses duress alarms to enable personnel to call for assistance in response to a threatening incident. Duress alarms must be monitored and initiate a response from monitoring services if activated.

Duress alarms must be installed at all customer service workstations or worn by personnel working in the front of house areas of service centres.

Fixed and portable duress alarms must be installed, programmed, tested and managed in accordance with the agency's Physical Security Technical Notes and design guidelines.

Closed circuit television (CCTV)

The agency uses CCTV to assist in the protection of staff, visitors and resources from criminal and/or anti-social behavior. CCTV also provides evidence to assist with the conduct of investigations and reviews including security incidents, criminal activities, fraud, code of conduct and contract management issues.

The agency installs CCTV in customer contact areas and non-customer contact areas, both internal and external to sites, where there is an assessed need.

The CCTV system must be appropriately managed and maintained to ensure the confidentiality, integrity and availability of the system, and compliance with relevant legislation.

Security guards

Security guards are deployed at both corporate and customer delivery sites within the agency. They provide deterrence against loss of information and physical resources and can provide a rapid response to security incidents. Stationary guards and guard patrols may be used separately or in conjunction with other security measures to mitigate identified risks. The agency has governance arrangements for the management and performance of security guards including Security Guard Standard Operating Procedures and Security Guarding Quality Assurance Framework.

Locks, Keys and Door Hardware

Locks are designed to deter and delay unauthorised access to information and physical assets. The PSPF requires the agency to use SCEC-approved locks and hardware in Zone Three to Zone Five. The agency may use either SCEC-approved locks or suitable alternate commercial locking systems in other areas.

All access points to the agency's facilities, including doors and operable windows, must be secured with locks and restricted key system in accordance with the agency's Physical Security Technical Notes and design guidelines.

Combinations and keys must be given the same level of protection as the highest classified information or most valuable physical asset contained in the area secured by the lock. Where the lock protects security classified information, keys must be stored in SCEC-approved key cabinets or containers.

Combinations, keys and electronic tokens must be changed where there is the possibility of compromise. Combinations must also be changed at six-monthly intervals. All security keys held and issued must be recorded in a key register.

Technical surveillance countermeasures

Technical surveillance countermeasures are implemented to protect security classified discussions from technical compromise. These countermeasures may include video recordings. The agency may also undertake technical surveillance countermeasure inspections:

- as part of programmed technical security inspections
- following a security breach involving the unauthorised disclosure of sensitive discussion.

Security zone certification and accreditation

As required by the PSPF, the agency must certify and accredit all areas within its facilities where security classified information and resources will be used, transmitted, stored or discussed, in accordance with the ASIO Technical Notes.

The Chief Security Officer (or delegate) is required to certify that the relevant control methods for the enforcement of physical security have been implemented and are operating effectively. For Security Zones 1 to 3, this includes a physical inspection and site certification, that shall be undertaken by an approved member of the Physical Security Infrastructure or Operations team. Site certification must be undertaken within 14 days of an agency facility being deemed fully operational at the conclusion of a new construction or following any minor works or capital works project that results in the provision of a new facility for the agency or changes to the layout and / or use of an existing facility.

For Security Zone 4, the site certification must be undertaken by an approved SCEC Consultant.

ASIO-T4 is the relevant certification authority for Zone Five security areas that are used to handle TOP SECRET security classified information, sensitive compartmented information or aggregated information where the aggregation of information increases its business impact level to catastrophic (5). The Australian Signals Directorate is the accreditation authority for Zone Five security areas used to secure and access sensitive compartmented information.

Security Zone accreditation involves compiling and reviewing all applicable certifications for the zone to determine and accept the residual risks. Approval is granted by the Accreditation Authority for the Security Zone to operate at the required level for a specified time period. The agency's Chief Security Officer has delegated authority to the Deputy Chief Security Officer (Agency Security Advisor – Physical and Personnel Security) to confirm the compliance and suitability of certification elements and accredit the agency's Security Zones 1to 4 inclusive. This position is held by the General Manager – Corporate and Cross Government Services.

Security zone certification is time limited. The assessment of compliance is specific to the role of the facility and the assets contained within the facility at the time of certification. This means the agency's facilities may require recertification from time to time. Security zone recertification and reaccreditation may be triggered by the following circumstances:

- expiry of the certification due to passing of time
  - for Zone Two security areas, being 10 years
  - for Zone Three to Zone Five, being 5 years
- changes in the assessed business impact level associated with the sensitive or security classified information or assets handled or stored within the zone
- significant changes to the architecture of the facility or the physical security controls.

ICT Facilities

The agency must certify and accredit the security zones for ICT sensitive and security classified information with an extreme business impact level.

Refer to the agency's Cyber Security Policies for further information on ICT security requirements.

Physical security outside the agency's facilities

When outside the agency's sites, official resources must be afforded the same level of protection as when located within the agency's facilities.

Personnel working away from the office, including undertaking home-based work, must continue to comply with the agency's physical security requirements to ensure the protection of agency information and assets.

Any non-agency facility (e.g. the private residence of agency personnel) are treated as Zone One areas for the storage and use of Commonwealth resources unless the agency has assessed and confirmed appropriate physical and procedural security measures are in place for a higher-level zone.

Incident management and reporting

Security is everyone's responsibility. Staff are responsible for the security of files, documents (both physical and electronic) and other official information that they use. A security incident can be an actual occurrence or threat that something will occur. This may include:

- harm to agency staff or visitors to agency facilities
- loss or compromise of sensitive or classified information, including customer information (including not following clear desk procedures)
- unauthorised access to agency facilities (including using someone else's IBA card to access facilities)
- damage, theft or loss of agency assets. (including failing to secure doors, gates or other access controls or the interfering or hindering of security infrastructure such as CCTV).

In addition to following agency security policies, staff, including contractors, have a responsibility to ensure they report security incidents.

Document control

Version	Date	Author (s)	Comments
1.0	February 2021	Physical Security	
1.1	October 2023	s 47F (1)	Added missing wording to title page
1.2	July 2025	Physical Security	Periodic review and amendment for 2025 PSPF release

Document endorsement

Status	Approved
Issue Date	July 2025
Issuing Authority	s 47F (1) , Director, Security Branch

servicesaustralia.gov.au

Australian Government
Services Australia

Official

Personnel Security Policy

July 2022

The Protective Security Policy Framework (PSPF) assists Australian Government departments or agencies to protect their people, information and assets, at home and overseas.

The PSPF articulates government protective security policy. It also provides guidance to departments or agencies to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security.

Effective personnel security facilitates the sharing of Australian Government resources, and is an essential mitigation tool to the threat posed by trusted insiders. To achieve the PSPF personnel security outcome, each department or agency implements the personnel security core requirements, supporting requirements, and guidance to ensure individuals are suitable to access Australian Government resources throughout all stages of their engagement with the department or agency.

Services Australia (the agency) aims to ensure individuals are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.

Contents

1 Personnel Security Policy

1.1 Policy overview

1.1.1 This Policy sets out what Services Australia (the agency) must do to meet the three core personnel security requirements of the Australian Government's Protective Security Policy Framework (PSPF).

1.1.2 Three core personnel security requirements of the PSPF are:

- Eligibility and Suitability of Personnel – we **must** ensure individuals are eligible and suitable to access to Australian Government resources (people, information and assets).
- Ongoing Assessment of Personnel – we **must** assess and manage the ongoing suitability of individuals and share relevant information of security concern, where appropriate.
- Separating Personnel – we **must** ensure that individuals leaving the agency have their access to Australian Government resources withdrawn and that they are informed of any ongoing security obligations.

1.1.3 This Policy applies to all individuals who require, or have non-public access to the agency's resources (people, information and assets).

1.1.4 For the purposes of this Policy, the term 'individual/s' is used for all ongoing and non-ongoing staff and all contractors, labour hire, consultants, third party providers and other government department or agency personnel.

1.1.5 This Policy and associated security procedures:

- **should** be read in conjunction with associated procedures on the Security Hub.
- provide a level of assurance to the agency regarding the eligibility and suitability of individuals requiring non-public access to agency and Australian Government resources.
- mitigate the risk of individuals exploiting or attempting to exploit their official access to the agency's resources or powers for unauthorised or improper purposes.

1.1.6 Individuals who hold, or are required to hold, an Australian Government security clearance **must** meet the extra requirements outlined in this policy under Section 5: Security Clearances.

1.1.7 Where this Policy uses the term 'security' it refers to protective security.

1.1.8 This Policy is specific to personnel security. Separate policies apply to physical security, security governance and information security.

1.2 Privacy, confidentiality and informed consent

1.2.1 The agency **must**:

- conduct personnel security activities in accordance with the Australian Privacy Principles.
- provide individuals with a privacy statement, which details how the agency collects, uses and discloses personal information (including sensitive information).
- obtain informed consent from individuals to collect, use and disclose personal information (including sensitive information) in regards to:
    - eligibility and suitability screening
    - ongoing suitability assessments
    - separation of individuals

- applications for security clearances
- management of security clearances and clearance holders
- revalidation of security clearances.

- only use the information for the purpose for which the informed consent has been given.
- only share an individual's personal information without informed consent, when it is permissible by law.

1.3 More information

1.3.1 For more information regarding this policy and associated procedures, please refer to the Security Hub.

1.3.2 For more information regarding this policy that is specific to security clearances, please refer to the Security Hub.

1.3.3 For definitions of security terms, please refer to the Security Hub.

2 Eligibility and suitability of individuals

2.1 Core requirements

2.1.1 The core PSPF requirement for eligibility and suitability of individuals states that agencies must ensure the eligibility and suitability of individuals who have access to Australian Government resources (people, information and assets).

This includes:

a) s 47E (d)

b)

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.

2.1.2 The agency's eligibility and suitability screening includes:

- eligibility and suitability checks (also known as pre-engagement checks)
- eligibility and suitability assessments based on the information obtained from the eligibility and suitability checks.

2.1.3 Any individual who requires non-public access to the agency's resources must complete and submit the necessary documentation to allow the agency to complete eligibility and suitability screening. This requirement applies even if the individual is a current or former employee of another Commonwealth Government agency, or the individual holds an Australian Government security clearance.

2.1.4 If an individual does not:

- participate in eligibility and suitability screening
- supply personal information requested in connection with the process
- satisfy any part of the agency's eligibility and suitability screening

the agency will not proceed with their engagement, and where the agency has already engaged the individual, the agency will terminate their contract or services.

2.1.5 Eligibility and suitability screening is only valid for a limited period and must re-occur at certain stages of an individual's engagement with the agency.

2.1.6 The agency's eligibility and suitability screening process must align with Australian Standard AS 4811-Employment Screening.

2.2 Eligibility and suitability checks

2.2.1 The agency conducts the following mandatory eligibility and suitability checks on an individual:

s 47E (d)

2.2.2 For certain positions within the agency, the individual may be required to undergo the following additional checks:

s 47E (d)

2.3 Eligibility and suitability assessments

2.3.1 The agency **must** conduct eligibility and suitability assessments on individuals, where their eligibility and suitability checks have revealed adverse results.

2.3.2 The agency's Personnel Security Team conducts the eligibility and suitability assessments and **should** (where applicable) involve:

s 47E (d)

-
-
- assessing the potential risks associated with granting an individual non-public access to the agency's or the Australian Government's resources
- applying mitigations to the potential risks.

2.4 More information

2.4.1 For more information regarding eligibility and suitability screening please refer to the Security Hub.

3 Ongoing assessment of individuals

3.1 Core requirements

3.1.1 The core PSPF requirement for ongoing assessments states that agencies **must** assess the ongoing suitability of individuals and share relevant information of security concern, where appropriate.

3.1.2 While eligibility and suitability screening and security clearance vetting provide an assessment of an individual's suitability at a point in time, ongoing awareness of changes in an individual's circumstances and workplace behaviours is essential to manage the risk of insider threat to the agency's resources.

3.1.3 The agency **must** assess and manage ongoing suitability to provide assurance that individuals:

- continue to meet the eligibility and suitability requirements which were established prior to commencement with the agency continue to meet an appropriate standard of integrity and honesty
- remain suitable to continue to access agency and Australian Government resources for the entire period of their engagement.

3.1.4 The agency **must** assess and manage ongoing suitability, which **should** include:

- periodic eligibility and suitability checks
- contact reporting obligations
- security incident reporting and follow-up
- reporting and managing changes in personal circumstances
- sharing information about an individual's ongoing suitability with relevant parties, internal and external to the agency.

3.1.5 In addition to the above, the agency **must** also assess and manage the ongoing suitability of individuals who hold a security clearance. This includes:

- conducting annual security checks
- monitoring compliance with certain security clearance conditions, if applicable.

3.1.6 For more information on Security Clearance holders, please refer to Section 5 below.

3.2 Manager responsibilities

3.2.1 Managers play an important role in supporting and assessing the ongoing eligibility and suitability of the individuals they manage.

3.2.2 The agency requires managers to address, manage and report on any behavioural concerns and changes in circumstances of the individuals they manage, that may pose a security risk to the agency, as soon as they arise. This includes considering the ethics, integrity and conduct of the individual.

3.2.3 Managers **must** conduct an annual security check on individuals who hold a security clearance. They can do this as part of the agency's annual performance management process.

3.2.4 Managers **must** report on any contacts that individuals may have with others who show a suspicious, persistent or unusual interest in their work or that of the agency, as or when they become aware of it.

3.2.5 Managers **must** report all security incidents that they witness or become aware of. For more information on reporting security incidents, please refer to Security Incident Reporting.

3.3 Periodic eligibility and suitability checks

3.3.1 The agency will conduct periodic eligibility and suitability checks for individuals who continue to access agency and Australian Government resources during their time with the agency.

3.3.2 Periodic eligibility and suitability checks **should** include:

- confirming and updating personal particulars such as address history, qualifications or employment history
- confirming adherence to, or completion of the agency's conditions of engagement
- s 47E (d)
- conflict of interest declaration
- confidentiality agreement
- specific agency checks, including staff integrity checks or customer integrity checks.

3.4 Contact reporting obligations

3.4.1 Under the Australian Government Contact Reporting Scheme, government personnel are required to report contact (either official or social) with representatives for foreign countries; extremist of subversive groups; criminal groups; or political or issue motivated groups or individuals.

3.4.2 Individuals **must** report to their manager and to Personnel Security any contact with or from:

- non-Australian citizens who seem suspicious, unusual or persistent in any way, or becomes ongoing.
- extremist or subversive groups, criminal groups, or political or issue motivated groups or individuals.
- former colleagues who show a suspicious, persistent or unusual interest in their work or that of the agency.
- people overseas who show a suspicious, persistent or unusual interest in their work or that of the agency.

3.4.3 Managers **must** report to Personnel Security as or when they become aware, of any contact individuals have, with or from:

- non-Australian citizens who seem suspicious, unusual or persistent in any way, or becomes ongoing
- extremist or subversive groups, criminal groups, or political or issue motivated groups or individuals

- former colleagues who show a suspicious, persistent or unusual interest in their work or that of the agency
- people overseas who show a suspicious, persistent or unusual interest in their work or that of the agency.

3.5 Personnel security incident reporting and follow-up

3.5.1 Individuals **must** report to their manager or to Security Support, all security incidents that they have witnessed or in which they have been involved.

3.5.2 Managers **must** report to Security Support as or when they become aware, of any security incidents that involve individuals who report to them.

3.6 Reporting and managing changes in personal circumstances

3.6.1 Individuals **must** report to their manager, or to Personnel Security, any changes in their personal circumstances.

3.6.2 Managers **must** report to Personnel Security, as or when they become aware, of any changes in personal circumstances for individuals who report to them.

3.6.3 The agency **must** collect, assess and manage any changes in personal circumstances for the agency's individuals.

3.7 Sharing information about ongoing suitability

3.7.1 The agency **must** share information of security concern, where appropriate.

3.7.2 The agency **must** share information of security concern, between managers, human resources areas, business integrity areas and security advisors, where appropriate.

3.7.3 The agency **must** share information of security concern with other government departments or agencies, where appropriate.

3.7.4 The agency **must** report any security concerns to ASIO (as defined in the *Australian Security Intelligence Organisation Act 1979*).

3.7.5 Information sharing may be limited by legislation, including the Australian Privacy Principles.

4 Separating individuals

4.1 Core requirements

4.1.1 The core PSPF requirements for separating individuals states that agencies **must** ensure that separating individuals:

- have their access to Australian Government resources withdrawn
- are informed of any ongoing security obligations.

4.1.2 Separating individuals include those who:

- voluntarily leave the agency
- have had their engagement terminated for misconduct or other adverse reasons
- transfer temporarily or permanently, to another Australian Government or agency (including machinery of government changes)
- take extended leave.

4.1.3 The agency **must** ensure that individuals continue to fulfil their obligations to safeguard agency and Australian Government resources, after they have left the agency. This limits the potential compromise of the integrity, availability and confidentiality of those resources. This includes:

- sharing relevant information, within the agency and with other government departments or agencies, where appropriate
- ongoing obligations and security debriefs
- removal of access
- risk assessments where normal separation procedures have not been carried out prior to separation
- risk assessments on individuals who are taking extended leave.

4.2 Sharing information within the agency

4.2.1 The relevant sanction delegate (or appropriate representative) **must** notify Personnel Security of any proposed and/or actual cessation of engagement resulting from misconduct or other adverse reasons (eg termination for cause or resignation following concerning conduct).

4.2.2 Security measures for high risk individuals will be based on a risk assessment, but may include:

- immediate suspension of duties
- immediate removal of all access to the agency's systems and facilities
- escorting the individual from the site.

4.3 Sharing information with other government departments or agencies

4.3.1 When individuals transfer to another Australian Government entity, the agency **must** provide the receiving entity with relevant security information about the individual. This information includes the outcome of any eligibility and suitability checks and assessments and any ongoing suitability assessments, as well as any concerns that were mitigated as part of those assessments.

4.3.2 The agency **must** advise other affected government entities if their interests or security arrangements could be affected, when an individual leaves the agency due to an incident (or if an incident is uncovered during the separation process).

4.4 Ongoing obligations

4.4.1 Prior to leaving the agency, the individual's manager **must** advise the individual of their continuing obligations under the *Crimes Act 1914*, *Criminal Code* and other relevant legislation, and obtain their acknowledgement of these obligations.

4.5 Withdrawal of access to agency resources

4.5.1 Prior to an individual's separation, the agency **must** recover from the individual, all ICT equipment, any physical assets, identity and building access cards, corporate credit cards and hardcopy official information.

- Managers **must** remove an individual's access to agency sites and ICT systems, when they leave the agency.

5 Security clearances

5.1 Core requirements

5.1.1 The agency **must** identify and record positions that require an Australian Government security clearance including the appropriate level of that security clearance.

5.1.1 Under the PSPF, if an individual occupies a position that requires ongoing access to security classified resources, the individual **must** hold a security clearance at the appropriate level. Security classified resources are defined by PROTECTED, SECRET and TOP SECRET information or systems that hold classified information, and classified assets.

5.1.2 An individual may also be required to hold a security clearance if they occupy a position requiring additional assurance about the integrity of the individual occupying that position.

5.1.3 Individuals cannot obtain a security clearance unless they are engaged in a role that requires a security clearance. Therefore, the agency cannot expect an individual to hold a security clearance prior to being selected for a designated role. Selection based on existing security clearance status is not merit based.

5.1.4 The agency **must** make employment decisions in accordance with the merit principle and cannot discriminate against individuals who do not hold a current security clearance where they indicate a willingness and ability to gain a security clearance prior to engagement.

5.1.5 The agency **must** recognise active Australian Government security clearances.

5.1.6 In exceptional circumstances, the agency may consider for the purposes of a security clearance:

- a citizenship waiver
- an uncheckable background waiver
- a short term security clearance
- a provisional security clearance.

5.1.7 s 47E (d)

5.1.8

5.2 Eligibility and suitability requirements for security clearance holders

5.2.1 Supplementary to the eligibility and suitability requirements in this policy, if the inherent requirements of a position require an individual to hold and maintain a security clearance, the agency **must** complete the individual's eligibility and suitability screening, prior to the agency sending a formal request for a security clearance to s 47E (d).

5.2.2 If the agency finds an individual is unsuitable, as part of eligibility and suitability screening, the agency **must** not seek a security clearance for the individual.

5.2.3 Where an individual holds a security clearance issued by an authorised vetting agency at the level required for the identified position (or higher), the agency may assume sponsorship of the security clearance. The agency will liaise with s 47E (d) egarding the sponsorship of the security clearance.

5.3 Ongoing assessment requirements for security clearance holders

5.3.1 Agencies **must** monitor and manage the ongoing suitability of its security clearance holders.

5.3.2 The agency (supplementary to the ongoing assessment requirements in this policy), **must** assess and manage ongoing suitability for its security clearance holders by:

- conducting annual security checks on individuals who hold a security clearance
- monitoring individuals who hold a security clearance.

5.4 Annual security checks

5.4.1 Agencies **must** conduct an annual security check on individuals who hold a security clearance.

5.4.2 The agency's annual security checks **should** include:

- confirming compliance with general security clearance obligations, as well as any specific clearance maintenance obligations associated with a conditional clearance.
- confirming compliance with the agency's security procedures
- reporting changes in circumstances
- reporting security incidents
- reporting suspicious, ongoing, unusual or persistent contacts
- completing security awareness training
- monitoring an individual's workplace behaviours to identify behaviours of concern.

5.4.3 The individual and their manager **must** conduct the annual security check.

5.5 Monitoring individuals who hold a security clearance

5.5.1 The agency **must** monitor and manage the ongoing suitability of individuals who hold a security clearance, including:

- collecting, assessing and sharing information of security concern.
- s 47E (d)
- conducting a review on individuals who hold a security clearance eligibility waiver.

5.6 Separating individuals requirements for security clearance holders

5.6.1 If an individual leaving the agency holds an Australian Government security clearance, or has access to sensitive or security classified information, their manager or Personnel Security (whichever is relevant based on the individual's clearance level) **must** debrief the individual.

5.6.2 s 47E (d)

5.6.3

5.7 Temporary transfer or secondment for security clearance holders

5.7.1 If an individual temporarily transfers or seconds to another government department or agency, the agency **should** consult with the gaining government department or agency, to determine whether to treat it as a separation for the purpose of security clearance sponsorship.

5.7.2 If the gaining government department or agency requires a higher level of security clearance or the individual's security clearance expires during the period of the temporary transfer, it is the responsibility of the incumbent government department or agency at the time to upgrade or renew the security clearance.

5.8 More information

5.8.1 For more information regarding security clearances please refer to the Security Hub.

6 Document control

Author	Date	Version	Reason
Personnel Security	January 2021	1.0	
Personnel Security	July 2022	1.1	Policy update

Document endorsement

Status	Approved
Issue Date	15 July 2022
Issuing Authority	NM Security, Deputy Chief Security Officer

Australian Government

Services Australia

servicesaustralia.gov.au