Australian Government

Department of Social Services

Department of Social Services Security Plan 2025-2027

Protecting our people, information and assets

DSS April 2025

Contents

Version Control

Version	Date Approved	Approved By	Summary of Changes
1.0	6 December 2021	Ray Griggs AO CSC (Secretary)	Final Approval
1.1	23 June 2023	Ray Griggs AO CSC (Secretary)	Review and update to reflect changes in the Department and its Portfolio. Inclusion of PSPF amendment.
1.2	24 June 2025	Michael Lye (Secretary)	Two-year security plan review and update to reflect 2024 PSPF release changes.

ARC Reference no: D25/793949

The Government's Protective Security Policy Framework

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

The Protective Security Policy Framework (PSPF) sets the Australian Government's minimum protective security standards to achieve effective and efficient secure delivery of government business, both domestically and internationally.

The 2024 PSPF release is set across six security domains and prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally. Application of the PSPF assures government that entities are implementing sound and responsible protective security practices and identifying and mitigating security risks and vulnerabilities.

PSPF Domains

- Governance – security planning, roles, training and reporting (Part One).
- Risk – enterprise risk management and third-party risk management (Part Two).
- Information – classification systems, information handling and data security (Part Three).
- Technology – cyber security (Part Four).
- Personnel – security vetting suitability assessments, access and separation (Part Five).
- Physical – security zoning requirements and site selection (Part Six).

The PSPF provides direction and guidance for:

- The Accountable Authorities of Australian Government entities, per the Public Governance, Performance and Accountability Act 2013 (PGPA Act).
- Entity Chief Security Officer, Chief Information Security Officer, security advisers and other named security officials.
- Service providers that provide services to Australian Government entities or are required to implement the PSPF according to relevant deeds or agreements.
- Those responsible for communicating security information to Australian Public Service (APS) employees, third-party service providers delivering services to Australian Government entities, and visitors to government facilities.
- Those working within, and for, the Australian Government, including APS employees, third-party service providers and contracted staff.

Entities must implement the PSPF requirements within their unique security risk environments.

The Department of Social Services (the department) provides security services for the Domestic Family Sexual Violence Commission and the National Commissioner for Aboriginal and Torres Strait Islander Children and Young People under Memorandum of Understandings, in accordance with the department's policies and procedures.

PSPF Annual Reporting

Under the PSPF, the department reports on security each financial year to our Minister and the Department of Home Affairs. The annual PSPF reporting process provides assurance to Government that entities are implementing sound and responsible protective security practices, and that security risks and vulnerabilities are being identified and mitigated.

Our Security Objective

Our objective is to protect our people, information, and assets so that the department can deliver on our mission to improve the wellbeing of individuals and families in Australian communities.

Our Security Goals

Our security goals are aligned to the six security domains contained within the PSPF.

Governance

Manage security functions and support a positive security culture ensuring clear lines of accountability, sound planning, assurance and review processes, and reporting.

- The department's security functions are managed to align with the requirements set within the PSPF.
- The department's security governance processes support the development, implementation and delivery of security function compliance including annual PSPF reporting requirements.

Actions and Key Performance Indicators included in the Security Plan and security related actions are reported to the Security Governance Committee.

Risk

Management of security risks form part of the entity's enterprise risk management framework, which is the set of components and arrangements in place to appropriately manage the entity's risks.

- The department's risk tolerance is currently 'low', based on the type of information the department handles and the assets we use to deliver our work.
- The department's Security Plan identifies risks which are reviewed on a 2-year basis, or as required, with material changes to the Security Plan reported to the Secretary through the Chief Security Officer.

Information

Maintain the confidentiality, integrity and availability of all official information, including maintenance of the privacy of information.

The department collects and manages a range of information, including sensitive personal information relating to individuals, classified as official information or above.

The department provides 'protected' advice to the Government and maintains financial information relating to payments and grants. Appropriately safeguarding this information, including ensuring the suitability of personnel who have access to it, is critical.

Technology

The department works with Services Australia to ensure that appropriate controls are in place to protect the department's ICT systems and information. This includes the hardening of the ICT network and applications, and the implementation of controls to meet the Australian Cyber Security Centre's (ACSC) Essential Eight Maturity.

The department also works closely with Services Australia to manage and mitigate cybersecurity threats and risks and responds to cybersecurity events when these occur.

Personnel

Ensures employees and contractors are assessed as suitable to access Australian Government resources and meet an appropriate standard of integrity and honesty.

- The department promotes a positive security culture and provides annual mandatory security awareness training, to all staff and contractors.
- The department's Personnel Security Policy sets out the requirements for implementing personnel security measures for the department to align with the requirement set within the PSPF.
- All staff and contractors are required to hold, at a minimum, a Baseline security clearance prior to commencement and undergo:
  - Identity verification using the Document Verification Service.
  - Suitability checks including a Nationally Coordinated Criminal History Check.
- The department has established a Designated Security Assessed Positions (DSAP) register.
- All staff are required to complete an annual security health check to report any changes in their circumstances that may impact their ability to maintain a security clearance.

Insider Threat

- The Department's Insider Threat Program is being developed in accordance with the PSPF 2024 Release and will be implemented by mid-2025.
- Insider threat is when an insider intentionally or unintentionally uses their access to conduct activities that could cause harm or negatively affect an entity or its operations.
- The Protective Security Section will have responsibility for the day-to-day operation of the Insider Threat Program and will have the lead role in the identification, analysis, prioritisation, and management of insider threat concerns within the Department.

Physical

Provide a safe and secure physical environment for our people, information, and assets.

- Many staff are now working from home on a regular basis under the Flexible Working Arrangements Policy. Additional corporate communication and security advice is provided to support staff working from home reminding staff to be vigilant of their surrounds and protect departmental assets in their care.
- All departmental facilities are certified to the appropriate Security Zone rating and accredited by the Agency Security Advisor (every two years). Individual risk assessments are conducted for each site in accordance with the PSPF.

s 47E(d)

[redacted]

Business Continuity

The department's Security Plan provides provisional guidance for security incident management and aligns with requirements outlined in the Australian Government's Protective Security Policy Framework. Contingency planning and protection strategies for managing security incidents are also outlined in the Security, Business Resumption Plan.

The department's Business Continuity Plan provides guidance for managing internal and external incidents that impact its core business, including critical business processes. The department's Critical Incident Response Team outlines senior personnel responsible for leading the agency's response during a significant incident or business disruption. Critical business processes are annually endorsed by the department's Executive Management Group and reflect core deliverables the agency must aim to uphold and continue to deliver during significant incidents or business disruptions. The department's current list of critical business processes (functional and seasonal) are at (**Appendix 3)** and are supported by branch level Business Resumption Plans and outline critical personnel, key resources, system dependencies and supporting protection strategies.

Our Security Environment

Security risk management is everyone's responsibility. It is fundamental to protecting our people, information, and assets, to allow the department to deliver on the Government's priorities.

The approach to security risk management is consistent with the department's Enterprise Risk Management Framework.

Australia continues to face a complex and evolving cyber threat environment increasing opportunities afforded to malicious actors, the activities of cybercriminals and foreign interference. These threats present a high risk to the Australian government and its agencies with an increasing amount of phishing and ransomware attacks specifically targeting user credentials and personal information held by agencies.

In 2020, the controls that constitute the Australian Cyber Security Centre's Essential Eight were significantly strengthened in response to this threat environment. These changes have resulted in enhanced measures and additional requirements to achieve the maturity levels of previous years.

The COVID-19 pandemic transformed the way Australians work. The department's flexible working arrangement policy now supports regular working from home arrangements for departmental staff. This altered the security posture of the department and continued heightened risks for information management, and IT cyber risks, including phishing scams.

To raise staff security awareness the department provides, through corporate communications, guidance to staff on home-based work, including security awareness training and effective use of IT devices and internet access. Security information is also provided for staff on the Protective Security STAFFnet page and regular STAFFnet articles and digital signage.

Our People

Our staff work in positions of high trust and are responsible for providing policy advice to Government including designing and administering programs that account for approximately one-quarter of the Australian Government budget.

The department's people, information, assets, and resources are dispersed across a number of different locations. This includes buildings where the department is responsible for the control of the security environment (wholly or partially leased premises); collocated offices where the department operates within another agency's secure environment; and community settings (urban, regional, remote) where staff work outside of an office environment.

Personnel (staff, contractors, consultants) undergo a Nationally Coordinated Criminal History Check, as required, identity verification, and are required to hold, at a minimum, a Baseline security clearance prior to commencement with the department.

The department aims to ensure that our staff are protected from harm at work and in the administration of their duties and are committed to fostering a culture where security risk management is recognised as everyone's responsibility.

Our Information

The department collects and manages a range of information, including sensitive personal information relating to individuals, classified as official information or above. The department also provides 'Protected' advice to the Government and maintains financial information relating to payments and grants. Appropriately safeguarding this information, including ensuring the suitability of personnel who have access to it, is critical.

The department requires all staff and contractors must hold, at a minimum, a Baseline security clearance to access information and or ongoing access to Commonwealth resources under the department's control.

The department operates within a Protected IT network and desktop environment.

ICT services are operated as a shared service by Services Australia, as outlined in the Services Schedule for ICT Shared Services.

- The department's cyber security capability is provided by Services Australia under a Shared Services arrangement, however overall accountability of cyber security remains with the department under the Chief Security Information Officer, who is supported by the department's cyber security team.
- Cyber security receives the appropriate level of managerial oversight through joint DSS/Services Australia governance mechanisms, including the Joint Services Management Committee (JSMC) and the SES level Strategic Cyber Security CISO Board. The Strategic Cyber Security CISO Board provides strategic direction and coordination across entities regarding ICT security issues.
- In conjunction with Services Australia, the department has established cyber security policies, procedures and standards that include specifying that systems processing sensitive or classified information must achieve the necessary authority to operate (or accreditation) before they are used, and they are subject to penetration testing as soon as practical and possible in a project's life cycle and ongoing at appropriate intervals.
- The department continues to work collaboratively with Services Australia to strengthen and enhance its information and technology networks against cyber threats in accordance with the Information Security Manual (ISM).
- The Australian Cyber Security Centre (ACSC) produces the ISM. The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

Our Assets

The department leases and purchases a range of assets to enable us to deliver our responsibilities. This includes, security systems and equipment, property and facilities, office furniture, vehicles, and office consumables. ICT operating environment and equipment is provided by Services Australia under the shared services arrangement.

Security Risk Appetite

The department's Enterprise Risk Management Framework guides how we undertake risk management and risk-based decision making across the department. A risk-based approach to how we plan and make decisions also helps us to focus on the things that matter and to prioritise the allocation of resources across multiple activities in a way that is methodical, efficient, consistent, and repeatable.

The Accountable Authority has determined the risk appetite for security risk as being 'low', based on the type of information we deal with and the assets we use to deliver our work.

The department's Security Risk Management Plan (**Appendix 2**) identifies the department's risks in accordance with the PSPF and details the controls and treatments in place to mitigate them.

Threat Assessment

We face a number of possible threat sources with the potential to cause loss and damage to our information and assets, or to cause harm to people. These threats have been identified consistent with the nature of the department's work, the impact of the threat, current controls, and security events that have occurred or are likely to occur.

The Incident Management Escalation Framework (**Appendix 1**) provides a scalable approach to measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level. The Physical Security Policy provides further guidance on incident escalations and responsibilities.

Security Goals	We will:	Key performance Indicator:
Governance **Manage security risks and support a positive security culture in an appropriately mature manner ensuring clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.**	Two yearly review and update the Security Plan and associated Security Risk Assessment for the Secretary's approval.	The Security Plan, Security Risk Assessment, and associated security risk mitigations are approved by the Secretary.
	Monitor our performance against the actions identified in the Security Plan. Performance reporting includes number of security incidents and staff participation in mandatory annual security training. Use information to improve compliance with the Security Plan 2025-2027.	Security performance reported to the Security Governance Committee. Improvements in compliance with security requirements noted between reporting periods.
	Provide mandatory security awareness training to increase the department's awareness and understanding the *Protective Security Policy Framework* and their role in protecting our people, information and assets.	95% of staff complete the security awareness training by 31 December annually.

Security Goals	We will:	Key performance Indicator:
Information Security **Maintain the confidentiality, integrity and availability of all official information.**	Undertake a rolling program of clear desk checks and information security briefings across all facilities to assess: • whether information classification markers are being appropriately applied to the department's information asset holdings • whether the department's information asset holdings are appropriately secured	100% of the department's workstations are subject to a clear desk check annually.
	Undertake a rolling twelve-month password reset program for all security containers and ensure the custodians of security containers are aware of their obligations to protect the department's information.	100% of security containers are password reset every twelve months.
	Manage the handling of hard copy security classified materials during transfer processes. This includes: • decommissioning assets that contain security classified information to ensure they no longer contain classified material (security containers and offices) Transfer hard-copy classified materials using 'safe hands' protocols – inspection, recording, and physical transfer with acknowledgement of receipt.	100% of security containers and offices decommissioned are physically inspected to ensure they are empty and signed off by the Branch Manager, responsible for the Security function, or in their absence the Agency Security Advisor. 100% of security classified documents are recovered or handed over to new owners using 'safe hands' protocols.
	Work with Services Australia to: • progress risk-based, cyber system accreditation of the department's ICT infrastructure and systems • ensure ongoing compliance with the ACSC Essential Eight mitigation strategies and increase the department's maturity ratings where possible • educate staff on information security risks to the department and the importance of their role in protecting	Implementation of ACSC Essential Eight mitigation strategies to uplift cyber maturity and improve maturity towards Maturity Level 2. Cyber system accreditation achieved and maintained on the network infrastructure and high-risk systems. Cyber and information security awareness training and educational material is available to all staff.

Security Goals	We will:	Key performance Indicator:
	the department's information and data assets	Targeted routine penetration testing carried out annually or whenever major system architecture modifications have been undertaken.

Security Goals	We will:	Key performance Indicator:
Personnel Security **Ensure employees and contractors are suitable to access Australian Government resources and meet an appropriate standard of integrity and honesty.**	Ensure all personnel requiring access to the department's resources have undergone (and cleared) suitability, identity and criminal history checks, and hold, and maintain (as a minimum) a Baseline security clearance.	100% of contractors and APS staff (without security clearances) requiring access undergo a Police Record Check (or equivalent) prior to engagement. 100% of personnel hold a security clearance, or have been granted appropriate access, in accordance with the PSPF, while awaiting grant of their security clearance.
	Manage the ongoing suitability of personnel: • Conducting security checks with all personnel annually • Reviewing all eligibility waivers annually	100% of staff complete security health check by 30 June annually. 100% of waivers reviewed by 30 June annually.
	Debrief all separating personnel who have access to security classified information and advise them of their continuing obligations under the *Crimes Act 1914*, *Criminal Code Act 1995* and other relevant legislation, and obtain the person's acknowledgement of these obligations.	100% of separating personnel with Positive vetting or Compartmental briefings, who have accessed sensitive or security classified information, acknowledge their obligation by completing an online or in person debrief. The department will endeavour to debrief all separating personnel who have accessed sensitive or security classified information, through the completion of an online debrief. For those the department cannot debrief, advice is provided to the relevant vetting agency identifying any security issues or concerns. The department's Designated Security Assessed Positions Register (DSAP) is up to date and reflects the current staffing establishment.

Security Goals	We will:	Key performance Indicator:
Physical Security **Provide a safe and secure physical environment for our people, information, and assets.**	Every two years undertake, or as the threat environment changes, certification and accreditation including individual risk assessments for all facilities and Security Zones.	Identified risks are mitigated to as low as possible in accordance with security risk tolerance. All Security Zones are certified and accredited against requirements specified in the ASIO Tec notes for secure facilities every two years and certified as compliant by the Agency Security Advisor. All Zones are monitored 24/7 by the Enid Lyons building on-site guard force and external Security Monitoring centre.
	Undertake a rolling twelve-month security asset audit and maintenance program.	100% of security assets are sighted. 100% of assets in use meet Security Construction Equipment Committee (SCEC) standards.
	Conduct travel briefings for staff travelling off-site for work or working in high-risk environments (remote communities, service providers, hostile or highly political community environments).	Staff are briefed and familiar with standard operating procedures on working in high-risk environments.

Security Roles and Responsibilities

Security roles and responsibilities span all levels of the department. Everybody has a role to play in protecting our people, information and assets.

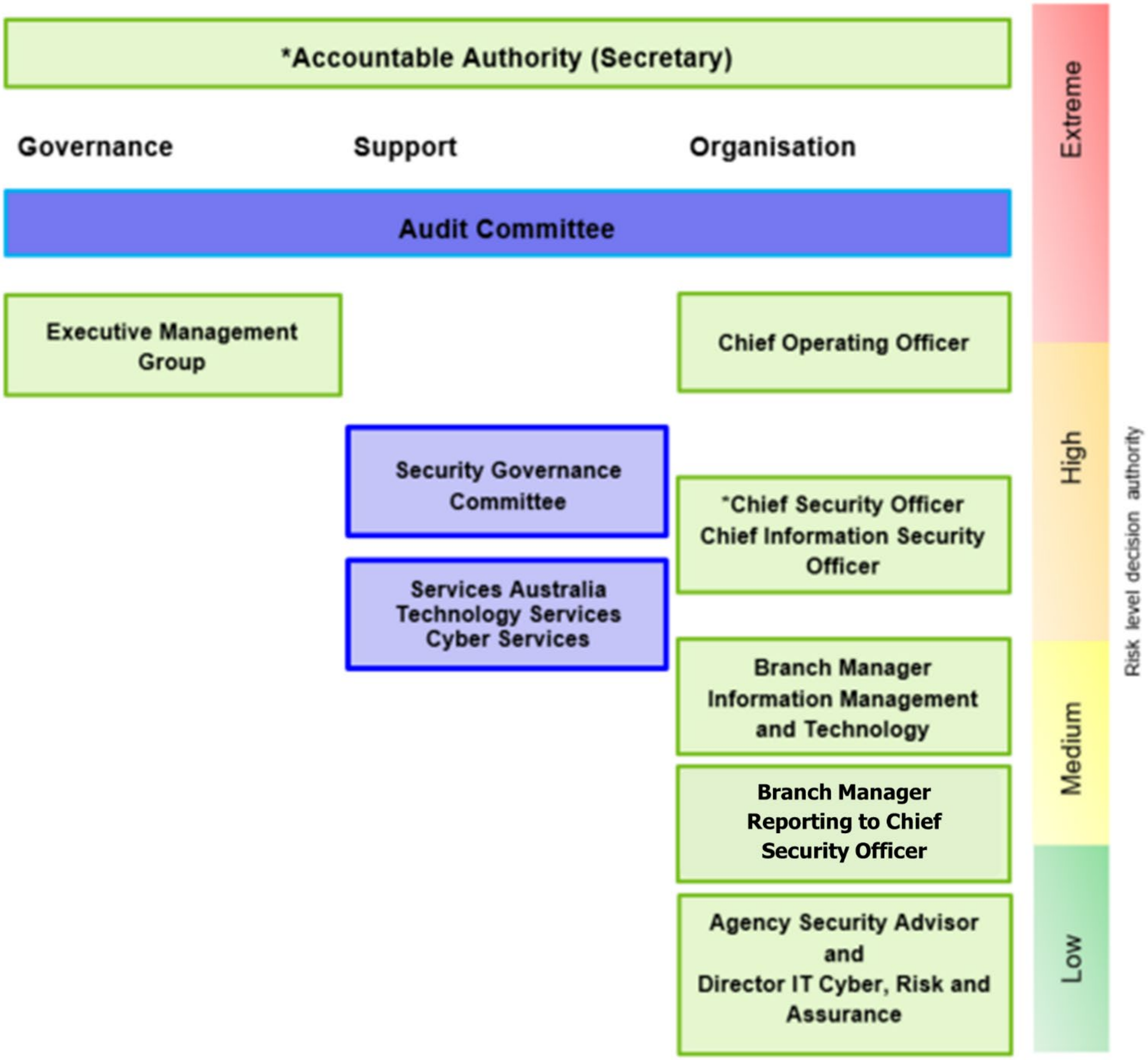
Roles	Responsibilities
The Secretary	The Secretary is the Accountable Authority under the requirements of the *Protective Security Policy Framework,* and is responsible for: • determining the department’s tolerance for security risks • managing the security risks in the department • considering the implications that risk management decisions have on other entities, and sharing information where appropriate
The Chief Security Officer and Chief Information Security Officer	The Chief Security Officer (CSO) role has been delegated to the Group Manager, Corporate and Government Services. The Chief Information Security Officer (CISO) role has been delegated to the Branch Manager, Chief Information Officer Branch. The Group Manager responsible for the department’s security function supports the overall security posture for the department. All are responsible for: • supporting the Accountable Authority to ensure the safety of the department’s people, information, and assets • establishing effective procedures to achieve security outcomes that are consistent with the PSPF, ISM and other Australian Government policies and legislative requirements • managing the department's response to security-related incidents and emergencies • fostering a positive security culture where personnel understand their responsibilities to manage security risk • ensuring information and security awareness training programs are in place so personnel understand their security obligations • establishing security performance measures to monitor and improve security maturity, and address security risks • disseminating and managing intelligence and threat information in the department • overseeing preparation of the entity's annual security report to accurately reflect its security maturity position and detail how it is addressing areas of vulnerability

Roles	Responsibilities
The Agency Security Advisor and Director IT Cyber, Risk and Assurance	The Agency Security Advisor and Director IT Cyber, Risk and Assurance support the CSO and the CISO and are responsible for: • identifying and managing security risks • ensuring security plans and procedures are effective in achieving specified security outcomes • monitoring the department’s security systems • providing advice on security-related issues • ensuring the department has a secure physical environment for official resources, including liaising with and managing security contractors • developing and conducting security awareness training • managing the eligibility and ongoing suitability of personnel • preparing security reports, and assisting with gathering information to meet annual security reporting obligations • coordinating and conducting security reviews, and being accessible for personnel to discuss security issues or concerns
Managers and Supervisors	Managers and Supervisors are responsible for: • positively influencing the protective security behavior of personnel (staff, contractors, consultants) • considering security risks as part of the annual business planning cycle • ensuring that staff undertake annual security training, adhere to clear desk procedure, and manage information in accordance with security classification requirements

Roles	Responsibilities
All personnel, including staff, contractors and consultants.	All personnel, including staff, contractors and consultants are responsible for: • understanding, applying, and complying with, the department's security policies • identifying, escalating, and where appropriate, managing security risks • undertaking security awareness training annually • undertaking a security health check annually • reporting security incidents • maintaining a security clearance, including reporting any changes in circumstances • managing information in accordance with security classification requirements • maintaining information in accordance with the clear desk procedure • protecting departmental assets while the asset is out of the office

Security Governance

Table 1: Department of Social Services Security Governance Structure



*Accountable Authority (Secretary)
Governance
Support
Organisation
Audit Committee
Executive Management Group
Chief Operating Officer
Security Governance Committee
Services Australia Technology Services Cyber Services
*Chief Security Officer Chief Information Security Officer
Branch Manager Information Management and Technology
Branch Manager Reporting to Chief Security Officer
Agency Security Advisor and Director IT Cyber, Risk and Assurance
Extreme
High
Medium
Low
Risk level decision authority

* Denotes positions mandated under the *Protective Security Policy Framework*

More information

For more information, please contact the Protective Security Section on s 22 or email security@dss.gov.au

Australian Government
Department of Social Services

Physical Security Policy

Policy information	Details
Policy No:	DSSCORP-046
Purpose:	To set out the department's policies relating to Physical Security
Category:	Corporate
Applicable to:	All staff, including contractors, consultants and visitors
Relevant Authority:	Chief Security Officer Department of Home Affairs
Related Documents:	Department Security Plan 23-25 Personnel Security policy Enterprise Risk Management Framework Australian Government Protective Security Policy Framework
Policy Statement:	The department is committed to implementing and maintaining the Australian Government's physical security requirements for the protection of the department's people, information and assets. This policy and associated guidelines detail those security requirements.
Approved by:	Chief Security Officer
Review Date:	March 2027
Policy Owner:	Property and Security Branch
First Issued:	September 2017
Document Change Control:	Amendments to v1.0 to reflect policy development on August 2018 – updated to v1.1 Amendments to v1.1 to review and update policy on August 2019 – updated to v1.2 Amendments to v1.2 to review and update policy on October 2021 – updated to v1.3 Amendments to 1.3 to review and update policy on March 2025 – updated to v1.4

Contents

1. Introduction

The department is committed to implementing and maintaining the Australian Government's physical security requirements for the protection of the department's people, information and assets. This policy and associated guidelines detail those security requirements.

This policy provides information on the implementation of physical security controls within the Department of Social Services (the department) and has been developed to provide a consistent and structured approach to the physical security arrangements for personnel accessing official and classified information and resources (people, information and assets). Physical security is the implementation of measures that; minimise or remove the risk of harm to people, information and physical asset, and resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

2. Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) in administered by the Department of Home Affairs. The PSPF undertook a significant revision under the 2024 PSPF release in November 2024. The revised PSPF articulates the government's requirements for protective security to be a business enabler that supports entities to work together securely, in an environment of trust and confidence. The PSPF is established as a policy of the Australian Government, which non-corporate Commonwealth entities are required to apply as it relates to their risk environment.

The PSPF sets out government protective security policy and supports entities to effectively implement the policy across the following domains:

- Governance
- Risk
- Information
- Technology
- Personnel
- Physical

The PSPF is applied through a security risk management approach, with a focus on fostering a positive culture of security within the entity and across the government.

3. Physical Security Core Requirements

The PSPF physical security mandatory requirements are defined in under the Physical domain and achieved through the implementation of four core requirements:

s 47E(d)

[redacted]

This policy is consistent with the requirements of the *Work Health and Safety Act 2011* and supports the departments compliance with the PSPF.

3.1. People

Personnel are central to the Department's operations. The protective security elements of the Model WHS Laws, and other appropriate legislative frameworks include:

- through threat and risk assessments identifying, protecting and supporting employees under threat of violence, while working in the office and away from office;
- reporting incidents;
- providing information, training and counselling to employees; and
- maintaining incident records and statements.

3.2. Information

PSPF details policy and guidance on classification and handling arrangements for protecting information resources.

Core requirements include:

s 47E(d)

[redacted]

The department is also required to comply with the Australian Privacy Principles as per the *Privacy Act 1988.*

As outlined in Principle 11:

- An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified. This requirement applies except where:
  - the personal information is part of a Commonwealth record, or
  - the APP entity is required by law or a court/tribunal order to retain the personal information.

-

3.3. Physical Assets

Physical assets are tangible items of value to the department. Applicable protections are based on the category of an asset and business impact levels (Appendix C) resulting from compromise, loss or damage of the asset.

Asset control is an effective process that helps to protect assets against theft, damage and loss.

4. Data & Privacy Breach Response

Data and privacy breach incidents may occur when personal or sensitive information under the Privacy Act 1988 is lost, used or disclosed incorrectly and gives rise to a breach of the Australian Privacy Principles.

The department has Data Breach Response Plan and Privacy Breach Response Plans in place to assist in the management of data and privacy breach incidents. The response plans detail the steps that need to be taken during the management of a breach.

In the instance of a potential breach, please refer to the Data or Privacy breach response plan resources on StaffNet.

This privacy incident report form will help assess the incident.

The assessment must be from either:

- the person involved in the incident.
- the person who identified the incident.

They must complete each part of the form.

They must send the completed form to the Privacy Team in the Legal Services Group. Email the form to InfoLaw@dss.gov.au as soon as possible (within 24-48 hours of identifying the incident).

Contact the Privacy Team if you need help.

5. Physical Security Measures

5.1. Physical Security Principles

Resource protection is achieved through using a combination of physical and procedural security measures to meet a threat environment. These measures should give suitable protection to assets and provide assurance to other agencies for information sharing.

Measures include:

s 47E(d)

[redacted]

s 47E(d)

[redacted]

5.2. Security In-Depth

Security in-depth is a multi-layered system where security measures are combined to support and complement each other making it difficult for an external intruder or a trusted insider to gain unauthorised access to information and assets. Successive layering or combinations of procedural and physical security measures include:

s 47E(d)

[redacted]

5.3. Security Zones

Physical security Zones are established in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed.

s 47E(d)

[redacted]

s 47E(d)

[redacted]

5.4. Clear Desk, Session and Screen Locking Procedures

PSPF details policy and guidance to prompt personnel to ensure that:

- no security classified information is left unattended on a desk (i.e. it is stored appropriately);
- ICT equipment (computers and media devices) is locked when not in use;
- electronic media and devices containing security classified information are secured;
- all portable and attractive items are secured;
- keys to classified storage devices are secured; and
- keys are not left in doors and drawers (at the end of the day or for an extended period of time).

Clear desk inspections are coordinated by the department’s Protective Security, Continuity and Emergency Management section in accordance with the Clear Desk Procedure (Appendix A).

5.5. Access Controls

Access control ensures that only authorised personnel, visitors, vehicles and equipment have appropriate facilities access and will only be granted to staff and contractors once a security clearance has been granted by the Australian Government Security Vetting Agency (AGSVA).

s 47E(d)

[redacted]

5.6. CCTV Systems

s 47E(d)

[redacted]

s 47E(d)

5.7. Secure Electronic Key Safes

s 47E(d)

5.8. Security Containers

s 47E(d)

5.9. Security Briefcases and Secure Satchels

s 47E(d)

5.10. Restricted Lock and Key Systems

s 47E(d)

5.11. Shredders and Secure Waste Bins

s 47E(d)

[redacted]

6. Assets

6.1. Physical Assets

Physical assets that require protection are identified based on the type of asset and considering their:

- monetary value;
- classification, whether classified in their own right or classified due to the information held on the asset, for example Information and Communications Technology equipment;
- attractiveness, not necessarily value; and
- cultural significance, regardless of monetary value.

6.2. Asset Control

The department's asset register supports identification of asset holdings and is an accountability mechanism that protects assets against damage and loss. Asset control includes:

- recording the location and authorised custodian;
- periodic auditing; and
- reporting requirements for the loss or damage of assets.

The department's Finance Group manages the asset register for the department.

6.3. Security of Information and Communications Technology Equipment

Management and storage of Information and Communications Technology (ICT) equipment will be in accordance with the ICT Acceptable Use Policy.

s 47E(d)

[redacted]

6.4. Audio Security

s 47E(d)

[redacted]

s 47E(d)

[redacted]

6.5. Working Flexibly Arrangements

The department has an obligation to provide a safe and secure work environment for its personnel. This includes all work undertaken personnel that is not conducted within the department's facilities.

Working away from the office includes;

- Working flexibly arrangements – working away from the office on a regular basis;
- out posting/co-location – working from a department state or regional office or from an alternative office space (non-department office under collocation arrangements);
- remote working – permanent working from home in a location remote from department offices; and
- work related travel.

Staff working under the department's Working Flexibly arrangements are required to:

s 47E(d)

[redacted]

Refer – Securely working away from the office and Transporting classified information

6.6. Residential Home Security

s 47E(d)

[redacted]

s 47E(d)

[redacted]

6.7. Out Posting Arrangements

s 47E(d)

[redacted]

6.8. Mobile Computing and Communications

Department mobile computing and communications include laptops, notebooks, tablets and mobile phones.

Care must be taken when using mobile computing and communication devices outside of department facilities. Further information on the use of mobile devices away from the office can be obtained from the department's Information Management and Technology Branch or via STAFFnet.

7. Security Risk Management Process

The department applies an enterprise-wide risk management approach regarding protective security in accordance with AS/NZS/ISO 31000:2018 (International Organization for Standardization – Risk management guidelines), HB 167:2006 (Standards Australia – Security risk management) and the department's Enterprise Risk Management Framework.

The department's security risk management methodology will:

- establish the scope of any security risk assessment and identify the people, information and assets to be safeguarded;
- determine the threats to people, information and assets, and assess the likelihood and impact of a threat occurring;
- assess the risk based on the adequacy of existing safeguards and vulnerabilities; and
- implement any supplementary protective security measures that will reduce the risk to an acceptable level.

s 47E(d)

[redacted]

s 47E(d)

[redacted]

8. Responsibilities

All managers and supervisors are expected to create and maintain an appropriate protective security environment that helps to:

- provide assurance that the department is well placed to reduce its exposure to security risks;
- identify their individual levels of security risk against the department's identified risk tolerance;
- achieve the mandatory requirements for protective security; and
- develop an appropriate security culture to securely meet the department's business goals.

Managing security risks proportionately and effectively enables the department to provide a safe and secure environment necessary for the protection of its critical assets and resources.

In the event of an identified threat of violence to staff, the department will take action to protect and support staff and where appropriate their family members and others. Details on action relating to such a threat is at **Appendix D**.

In an emergency situation staff should contact the relevant emergency services by dialling 000.

8.1. Accountable Authority

The Secretary as the Accountable Authority is answerable to the Minister and Government for the security of the department.

The Accountable Authority:

- determines the department's tolerance for security risks;
- manages the security risks of the department; and
- considers the implications risk management decisions have for other entities, and shares information on risks where appropriate.

8.2. Chief Security Officer

The Secretary has appointed Group Manager Corporate to the role of Chief Security Officer (CSO).

The CSO supports the Secretary by providing strategic oversight of protective security across governance, information (including ICT), personnel and physical security to assist continuous delivery of business operations. The CSO is responsible for fostering a culture where personnel have a high degree of security awareness.

8.3. Agency Security Advisor

The Agency Security Advisor (ASA) supports the CSO by*:*

- managing the PSPF requirements are applied throughout the department;
- ensuring appropriate department security plans, policies and procedures are in place;
- ensuring all personnel are aware of their security responsibilities;
- provide security advice to department Executive, managers and staff;
- reporting to the CSO on the security health of the department;
- provide annual security awareness training for all personnel;
- advising business areas of specific security requirements;
- conducting initial assessments into lapses of physical security, and if required, refer incidents for investigation; and
- maintain records of reported incidents.

8.4. Managers

- complete annual security awareness training and encourage personnel to complete this training;
- adhere to the department's physical security protocols to maintain the confidentiality, integrity and availability of information;
- understand the business impacts if information confidentiality is compromised;
- account for sensitive and/or classified information which is in their control;
- assume custodianship of a security container and secure contents according to physical security instructions and guidelines (where applicable);
- assist personnel to be aware of their physical security responsibilities in support of strengthening the department's security culture through training and provision of counselling for employees in need; and
- report any concerns regarding physical security to their respective managers, or the Agency Security Advisor.

8.5. All Personnel (staff, contractors, and consultants)

- complete security awareness training on engagement and annually;
- comply with the department's physical security protocols;
- understand the business impacts if information confidentiality is compromised;
- account for sensitive and/or classified information which is in their control;
- report any concerns regarding physical security to their respective managers and the Agency Security Advisor; and
- undertake appropriate processes when separating from the department.

9. Sanctions For Non-Compliance

Non-compliance of this policy may result in action being taken under one of the governing provisions listed below*:*

- *Public Service Act 1999* (Cth)
- *Crimes Act 1914* (Cth)
- Criminal Code (1995) (Cth)
- *Public Governance, Performance and Accountability Act 2013* (Cth)
- Reporting of security incidents to the Australian Government Security Vetting Agency.
- APS Code of Conduct

9.1. Security Incident Reporting

Staff involved in, or are aware of, a security incident have a responsibility to report these by completing and submitting a Security Incident Report within eForms.

10.More Information

For more information, please contact the Protective Security, Continuity and Emergency Management section, in the Property and Security Branch on
s 22 or email security@dss.gov.au.

Non-Compliance

Department personnel must observe all security requirements under their employment agreement, or contract of engagement, and the department's security governance and policies.

Department personnel will receive formal advice when a non-compliance is identified. The advice will be provided via email and will advise of remedial action required.

Repeat instances of non-compliance may be referred to Workplace Relations, People Services Branch.

14. APPENDIX D

Managing Security incidents

Security of the department’s staff is an ongoing priority. The Protective Security section engages closely with staff and managers to provide support to employees who may experience concerns for their safety in the workplace.

The effective handling and recording of security incidents are a fundamental commitment to providing a safe and secure work environment. Information gathered on security incidents allows the department to identify, protect and support employees under threat of violence based on a threat and risk assessment of specific situations.

Information gathered about security incidents may, if required, be shared with State Police authorities as appropriate, and internally (including with People Services Branch) where additional support is considered necessary.

Where an incident occurs where a physical asset or information is lost, misplaced or disclosed the data and or privacy breach response plans would be actioned to manage the incident response.

Data & Privacy Breach Response

As previously mentioned, in the instance of a potential breach, please refer to the privacy breach response plan resources on the Privacy Staffnet.

This privacy incident report form will help assess the incident.

The assessment must be from either:

- the person involved in the incident.
- the person who identified the incident.

They must complete each part of the form.

They must send the completed form to the Privacy Team in the Legal Services Group. Email the form to InfoLaw@dss.gov.au as soon as possible (within 24-48 hours of identifying the incident).

Contact the Privacy Team if you need help.

What is a Security incident?

A security incident for the purposes of this policy, is where a staff member or manager has concerns for their or their staff’s security in the workplace. This could be related to a personal circumstance, or duties undertaken as part of departmental roles.

Security support

s 47E(d)

[redacted]

Staff and managers should familiarise themselves with the Department's Escalation Policy.

Security working with People Services and Property may be able to offer additional support, on a case-by-case basis including:

s 47E(d)

[redacted]

Managers

Managers have an important role to play in security incident reporting. Their supervisory role makes it probable that they could be the first to detect a concern relating to staff safety. Detailed knowledge of their staff makes it likely they will become aware of any behaviour that may be of concern. Managers should ensure that security incidents, or concerns are reported to Protective Security or People Services as appropriate.

Reporting Incidents

All security related incidents are to be reported to Protective Security or People Services with the following details:

- time, date and location of security incident.
- type of incident
- description of the circumstances of the incident
- assessment of the possible impact on the staff member
- summary of immediate and/or long-term action taken
- point of contact.

Additional Information

Information relating specifically to the support available for employees experiencing family and/or domestic violence can be found in the Department's Domestic and Family Violence policy.

Australian Government
Department of Social Services

Personnel Security Policy

Policy information	Details
Purpose:	To set out the Department's policies relating to Personnel Security
Category:	Corporate
Applicable to:	All staff, including contractors, consultants and visitors
Relevant Authority:	Chief Security Officer Department of Home Affairs
Related Documents:	Department Security Plan 2025-2027 Physical Security Policy Enterprise Risk Management Framework Working with Children and Vulnerable People Suitability Assessment Policy Australian Government Protective Security Policy Framework
Policy Statement:	The Department is committed to implementing and maintaining the Australian Government's personnel security requirements for the protection of the Department's people, information and assets. This policy and associated guidelines detail those security requirements.
Approved by:	Chief Security Officer
Review Date:	March 2027
Policy Owner:	Property and Security Branch
First Issued:	27 November 2013
Document Change Control:	Amendments to v3.1 as directed by the CSO on 14 June 2022 – updated to v3.2 Amendments to v3.2 as directed by the CSO on 22 August 2022 – updated to v3.3 Amendments to v3.3 to reflect implementation of the AGSVA myClearance portal and process changes on 12 January 2023 – update to v3.4 Amendments to v3.4 to reflect reassignment of PSPF to the Department of Home Affairs and amendment to the terms of reinstatement for inactive security clearances – update to v3.5 Amendments to v3.5 to reflect PSPF Release 2024 and general policy review – update to v3.6 Amendments to v3.6 to reflect PSPF Direction 003-2025 – update to v3.7

Contents

1. Introduction

This policy provides information on the implementation of personnel security controls in the Department of Social Services (the Department) and has been developed to provide a consistent and structured approach to the personnel security arrangements for staff and contractors[1] accessing official and security classified resources (people, information and assets). Personnel security is the management of staff and contactors to assist in the protection of Australian Government resources and provides a level of assurance as to the honesty, trustworthiness, maturity, tolerance, resilience and loyalty of individuals who access Australian Government official or security classified resources.

The Protective Security Policy Framework (PSPF) is the overarching framework that Australian Government departments and agencies must comply with and is mandatory for non-corporate Commonwealth entities. It is applied through a risk management approach, with a focus on fostering a positive security culture across government.

To achieve the PSPF personnel security requirements the Department must ensure eligibility and suitability of staff and contractors who access the Department's official or security classified resources. All staff and contractors require a minimum Baseline security clearance prior to access the Department's IT systems and/or have unescorted access to the Department's facilities.

2. Personnel security core requirements

The PSPF Personnel Security mandatory requirements are defined in part 5 of the PSPF and are achieved through the implementation of the core requirements:

- eligibility and suitability of personnel (Pre-Employment Screening)
- vetting through the Australian Government Security Vetting Agency (AGSVA)
- ongoing assessment of personnel
- separating personnel.

2.1. Eligibility and suitability of personnel and security vetting

Pre-employment screening and security clearances ensure all staff and contractors are eligible and suitable for their roles. Under the PSPF, a person who is deemed eligible and suitable demonstrates integrity, trustworthiness and is not vulnerable to improper influence.

2.2. Adverse Findings

In accordance with the principle of procedural fairness, staff, contractors or applicants who are assessed by the AGSVA as potentially unsuitable to hold a security clearance will be given the opportunity to respond in writing before a final decision is made: In summary:

- They will be provided with a summary of the AGSVA's concerns related to their suitability to hold or retain a security clearance
- In their response they may provide information to:

[1] Contractor – Service provider, Labour hire contractor, Contractor, Consultant

- correct any errors of fact
- detail any special circumstances which they believe need to be taken into account
- offer further evidence relevant to the concerns which they believe need to be taken into account
- the concerns which may provide sufficient mitigation to grant or continue the security clearance.

Prior to a final decision by the AGSVA, the decision maker will review all the information, including the person's response.

2.3. Decision Review

If a person has received notification that their security clearance application is denied or revoked, in accordance with the PSPF they can ask for a review of the decision.

If they are an:

APS employee they have 3 review options:

- Primary review by the AGSVA – they have 120 days from the decision notification to request a review
- Secondary review by the Merit Protection Commissioner – if they are unsatisfied with the AGSVA review or the decision is not reviewable. They have 60 days from the decision of the primary review to make an application
- Lodge a complaint with the Commonwealth Ombudsman – the Ombudsman will generally only investigate if the other review processes have been completed.

Non-APS employee they have 2 review options:

- Internal review by the AGSVA
- Lodge a complaint with the Commonwealth Ombudsman – the Ombudsman will generally only investigate if the other review process has been completed.

2.4. Pre-Employment screening

Pre-employment checks provide the Department with assurance of a prospective employee's eligibility and suitability to access official information and resources. They include background and identity checks that:

- verify a person's identity using the Document Verification Service (DVS) or where the DVS is not available through a manual check
- confirm a person's eligibility to work in Australia
- obtain 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.

2.5. Security Clearances

A security clearance is a determination by the AGSVA that an individual is eligible and suitable from a security standpoint, to access security classified information by:

- considering a person’s integrity (i.e. the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Standard which are defined in the Australian Government Personnel Security Adjudicative Standard
- resolving any doubt about a person in the national interest.

2.6. Discrimination

The Department and any contracted service provider advertising employment vacancies are not to discriminate against those applicants who are not holders of a security clearance where they indicate a willingness to undergo a clearance process prior to employment.

2.7. Ongoing assessment of personnel

s 47E(d) [redacted]

2.8. Separating personnel

The Department’s and Australian Government resources can still be compromised after an individual has ceased employment or an engagement with the Department.

The Department’s processes for separating personnel includes:

s 47E(d) [redacted]

3. Pre-employment and Security Clearances

Pre-employment background and identity checks and a minimum Baseline security clearance **must be completed before** staff or contactors requiring access to the Department’s IT systems and/or unescorted access to the Department’s facilities are engaged.

All advertisements for vacancies and selection documentation must include the pre-employment check and security clearance as a condition of employment. The Department and any contracted service provider advertising employment vacancies are not to discriminate against those applicants who are not holders of a security clearance where they indicate a willingness to undergo a security clearance assessment process prior to employment.

Contracts with outsourced providers **must** include a clause stipulating that any contractor employee accessing the Department’s IT systems and/or requiring unescorted access to the

Department's facilities must undergo a pre-employment check and hold a minimum Baseline clearance. Security clearance costs incurred by the Department for outsourced providers are subject to cost recovery.

Additional background checks may be required for positions where risks have been identified or higher assurance of the position holder's integrity is required. These checks may include:

s 47E(d)
[redacted]

The Department may conduct further checks when the above checks raise security concerns about the applicant's suitability or eligibility to access official resources.

Security Clearance Levels

The 4 levels of Australian Government security clearance are:

Clearance Level	Information Accessible
Baseline Vetting (minimum requirement)	PROTECTED
Negative Vetting Level 1	PROTECTED, SECRET
Negative Vetting Level 2	PROTECTED, SECRET, TOP SECRET
Top Secret-Privileged Access Clearance (TSPA - Positive Vetting)	Permits access to information or resources at all classification levels including certain types of caveated, compartmented and code word information

Further details at Annex A.

3.1. Security assessed positions – minimum clearance levels

The Department has assigned security clearance levels to all positions. This requires the person occupying a position to obtain and maintain the required level of security clearance assigned to the position. This includes:

s 47E(d)
[redacted]

All advertisements for vacancies and selection documentation must include the required level of security clearance as a condition of employment.

s 47E(d)

3.2. Pre-employment checks where personnel do not have an active security clearance

The timeframe for pre-employment checks must be included in the assessment and engagement of staff and contractors. A Nationally Coordinated Criminal History Check (NCCHC) may exceed 10 business days and are unable to be escalated. For AGSVA timeframes, please refer to Timeframes | Australian Government Security Vetting Agency.

The NCCHC is a point in time check and is s 47E(d) from date of release. If the new starter has not commenced with DSS s 47E(d), a new NCCHC will be required. The department will not accept NCCHC's that have been initiated by a third-party entity, including Commonwealth agencies.

As part of the pre-engagement pack candidates are require complete an informed consent document. The informed consent allows the collection, use and disclosure of personal information for the purposes of pre-engagement security checks and assessing and managing eligibility and suitability to hold a security clearance. Informed consent documents are valid for a maximum period of s 47E(d) from the signature date.

s 47E(d)

3.3. Pre-employment checks where personnel have an active security clearance

Where incoming personnel have an active security clearance, the Protective Security Section will organise to transfer security clearance sponsorship to the Department. Once the AGSVA has sponsored the security clearance, identity documents verified, the member's NCCHC returned (with no adverse outcomes) and any declarations assessed, the Protective Security Section will authorise Recruitment to commence the on-boarding process.

3.4. Contractors and grants recipients who do not require security clearances

s 47E(d)

s 47E(d)

[redacted]

3.5. Pre-employment checks for personnel undergoing Machinery of Government changes

The Australian Public Service Commission, Machinery of Government provides guidance for Machinery of Government changes. The Guide recommends taking a whole-of-government approach while ensuring accountability and compliance with legislation and policy. Each Machinery of Government change will be treated separately; however, where possible and practical the Department will leverage off the pre-employment checks carried out by the losing agency.

The Department still requires staff or contractors to hold, at a minimum, a Baseline security clearance prior to accessing the Department's IT systems, information and having unescorted access to the Department's facilities.

3.6. Nationally Coordinated Criminal History Check revalidation

The National Police Checking Service Handbook confirms the NCCHC is a point-in-time check and the Department's decision makers are responsible for determining how long a NCCHC is to be accepted as 'valid'. The Protective Security Section is responsible for determining if a new NCCHC is required for personnel that have had a break in service.

The Commonwealth spent conviction scheme, outlined in Part VIIC of the *Crimes Act 1914* (Cth) (Crimes Act), is considered by authorities when completing a NCCHC. In some circumstances, these schemes do not apply, for example involving people who work with children and vulnerable groups. However, for the majority of the Department's staff the spent conviction scheme applies.

3.7. Clearance sponsorship

The Department will sponsor security clearances for the Department's staff and contractors who require access to sensitive or classified information for the performance of their duties and/or require unescorted access to the Department's facilities.

3.8. Security Clearance Aftercare

Aftercare is the maintenance of effective personnel security after a security clearance is granted. Its purpose is to identify anything of security concern, between periods of normal review, which affects an individual's suitability to hold a security clearance.

The Department requires:

s 47E(d)

[redacted]

3.9. Changes in personal circumstances

Staff and contractors are required to report any changes in personal circumstance to the AGSVA through submission of a Change of Circumstances Application within the myClearance portal. Additional information is available on the AGSVA's website.

3.10. Eligibility Waivers

To be eligible for an Australian Government security clearance, an individual must be an Australian citizen and have a checkable background.

The Secretary, as the accountable authority, in exceptional circumstances may approve an eligibility waiver to enable the security clearance process to proceed.

Further details at Annex B.

3.11. Certificate of Suitability

Staff from other Australian Government entities that require access to departmental resources under colocation or shared servicing agreements are required to submit a Certificate of Suitability to the Protective Security Section.

s 47E(d)

[redacted]

4. Insider Threat Program

4.1. Insider Threat

The Department's Insider Program is being developed in accordance with the PSPF 2024 release and will be implemented by mid-2025.

Insider threat is when an insider intentionally or unintentionally uses their access to conduct activities that could cause harm or negatively affect an entity or its operations.

An insider is a current or former personnel (including contractors) who has, or had, legitimate or indirect access to an entity's people, information, techniques, activities, technology, or resources. All APS employees are trusted to uphold the APS Values and comply with the APS Code of Conduct. They are therefore considered to be 'trusted insiders'. A trusted insider is commonly referred to as an insider.

A trusted insider may be acting on behalf of a foreign power, issue-motivated group, organised crime groups or violent extremist groups etc. either intentionally or unintentionally to gain access to official or security classified information.

Countering insider threat programs enable entities to identify and manage insider risk in a holistic and coordinated way.

s 47E(d)

[redacted]

s 47E(d)

[redacted]

5. Responsibilities

5.1. Accountable Authority

The Secretary as the Accountable Authority is answerable to the Minister and Government for the security of the Department.

The Accountable Authority:

- determines the Department’s tolerance for security risks
- manages the security risks of the Department
- considers the implications of risk management decisions for other entities, and shares information on risks where appropriate.

5.2. Chief Security Officer

The Secretary has appointed Group Manager Corporate and Government Services to the role of Chief Security Officer (CSO).

The CSO supports the Secretary by providing strategic oversight of protective security across governance, risk, information, technology, personnel and physical security to assist continuous delivery of business operations. The CSO is responsible for fostering a culture where personnel have a high degree of security awareness.

5.3. Agency Security Advisor

The Agency Security Advisor (ASA) supports the CSO by:

- managing the Protective Security Policy Framework requirements
- ensuring all staff are aware of their personnel security responsibilities
- reporting to the CSO on the security health of the Department
- provide annual security awareness training for all staff and contractors
- advising business areas of specific personnel security requirements
- conducting initial assessments of personnel security incidents/breaches, and if required, refer incidents for internal investigation.

5.4. Managers

Managers are required to:

- monitor the personnel security health of their staff and contractors
- report any concerns regarding personnel security to the ASA
- advise the Protective Security Section of the separation or transfer of staff and contractors through appropriate processes

- notify the CSO, through the ASA of any proposed terminations of employment where there are conduct concerns
- ensure that all recruitment (staff) and engagement (contractors) processes adhere to pre-employment and security vetting requirements.

5.5. All personnel (staff, contractors)

All personnel are required to:

- comply with pre-employment screening and eligibility check processes
- report any changes of circumstances to the AGSVA, and their manager if appropriate, as soon as possible after the occurrence
- comply with AGSVA processes
- adhere to individual personnel security clearance responsibilities and obligations
- complete security awareness training on engagement and annually
- comply with the Department's personnel security protocols
- report any concerns regarding personnel security to their respective managers and the ASA
- undertake appropriate processes when separating from the Department.

5.6. Social media platforms

- As security clearance holders, all personnel (staff, contractors) must adhere to PSPF Requirements and Directions issued by the Secretary of the Department of Home Affairs. PSPF Direction 003-2025 requires that personnel must not disclose information that identifies or alludes to their access to security classified materials, including the level of security clearance held on social media platforms. This includes social networking services such as LinkedIn.

6. Sanctions for non-compliance

Non-compliance with this policy may result in action being taken under one of the governing provisions listed.

- *Public Service Act 1999* (Cth)
- *Crimes Act 1914* (Cth)
- *Criminal Code (1995)* (Cth)
- *Public Governance, Performance and Accountability Act 2013* (Cth)
- reporting of security incidents to the AGSVA
- APS Code of Conduct
- *National Anti-Corruption Commission Act 2022*

7. More Information

For more information, contact the Protective Security Section:

✉ Security@dss.gov.au

☎ s 22 [redacted]