PSPF Release 2025 – Changes Summary

A summary of the changes introduced in PSPF Release 2025 is provided below.

Governance Domain

Location	Subject	Requirement or Table	Change
Section 2.3	Chief Information Security Officer	0011	A Chief Information Security Officer is appointed to oversee the entity's cyber security program and the cyber security for the entity's most critical technology resources~~, including information technology and operational technology~~
Section 2.3	Chief Information Security Officer	0013	The Chief Information Security Officer is accountable to the Accountable Authority for cyber security risks and how the entity's cyber security program is managing these risks.
Section 3.6.3	Externally Reportable Security Incidents and Referral Obligations – Significant Security Incidents (reporting obligation)	Table 2	• Significant security incidents. • Lessons learnt from any incidents, investigations, reports or reviews relating to the incident. • Potential or identified foreign ownership, control or influence risks identified during the procurement process.

Risk Domain

Nil changes.

Information Domain

Location	Subject	Requirement or Table	Change
Section 9.3.1	Protections and Handling Requirements for Physical information – Inside Entity Facilities – Access Control	Table 4	OFFICIAL: Sensitive Need-to-know principle: Yes. Security clearance: Nil, employment screening only for entity personnel. Agreement or arrangement for non-government stakeholders, unless the entity is returning or responding to information provided by a non-government stakeholder, or their authorised representative, which the government entity would subsequently classify as OFFICIAL: Sensitive on receipt (as the government originator).

Location	Subject	Requirement or Table	Change
Section 9.3.1	Protections and Handling Requirements for Physical information – Inside Entity Facilities – Access Control	Table 4	PROTECTED, SECRET and TOP SECRET Class A shredder or ASIO-T4 approved destruction method.
Section 9.3.1	Protections and Handling Requirements for Physical information – Travelling Outside of Australia (international travel)	Table 8	SECRET Not recommended. If required, retain as carry-on luggage in a diplomatic bag and retain in the custody of a laissez-passer, Australian Diplomatic or Australian Official passport holder. If airline requires carry-on baggage to be checked at the gate, do not travel.
Section 9.3.2	Protections and Handling Requirements for Government-issued Mobile Devices – Government-Issued Mobile Devices – Inside Entity Facilities	Table 9	Need-to-know principle: Yes. Security clearance: Nil, employment screening only, unless the entity is returning or responding to information provided by a non-government stakeholder, or their authorised representative, which the government entity would subsequently classify as OFFICIAL: Sensitive on receipt (as the government originator).
Section 9.5	Security Caveats and Accountable Material	0064	Security caveats are clearly marked as text and only appear in conjunction with a security classification ~~of PROTECTED or higher~~.
Section 12.1.3	Sharing with Non-Government Stakeholders	0077	An agreement or arrangement, such as a contract or deed, that establishes handling requirements and protections, is in place before security classified information or resources are disclosed or shared with a person or organisation outside of government, unless the entity is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the government entity subsequently classified as OFFICIAL: Sensitive.
Section 12.3	International Information Sharing	0080	Australian Government security classified information or resources bearing the Australian Eyes Only (AUSTEO) caveat is never shared with a person who is not an Australian citizen, even when an international agreement or international arrangement is in place, unless an exemption is granted.

Technology Domain

Location	Subject	Requirement or Table	Change
Section 13.2	Technology Estate *(replaces Network Architecture)*	0211	A Technology Asset Stocktake and Technology Security Risk Management Plan is created to identify and manage the entity's internet-facing systems or services to ensure continuous visibility and monitoring of the entity's resource and technology estate.
Section 13.3	Technology System Authorisation – Gateways	Table 21	• TOP SECRET requires an ASD assessment. • SECRET and below require an IRAP Assessment.
Section 13.3	Technology System Authorisation – Gateways	0088	The technology system is authorised to the highest security classification of the information and data it will process, store or communicate ~~communication~~.
Section 13.10.1	Artificial Intelligence *(new section)*	N/A	Introduces new policy content and references relevant existing PSPF Requirements that apply: • PSPF Requirement 0039 • PSPF Requirement 0040 • PSPF Requirement 0046 • PSPF Requirement 0049 • PSPF Requirement 0062 • PSPF Requirement 0086 • PSPF Requirement 0087
Section 13.10.2	Quantum Technologies and Quantum Computing *(new section)*	0212	Approved post-quantum cryptographic encryption algorithms are used for newly procured cryptographic equipment and software in accordance with the Information Security Manual's guidelines for cryptography.
Section 13.10.3	Connected Peripheral Technologies *(new section)*	N/A	Introduces new policy content.
Section 14.1	Cyber Security Strategy	0098	A cyber security strategy and uplift plan is developed, implemented and maintained to manage the entity's cyber security risks in accordance with the Information Security Manual and the Guiding Principles to Embed a Zero Trust Culture.
Section 14.1	Cyber Security Strategy	0213	The Chief Information Security Officer reports on the entity's cyber security risk at each meeting of the Audit Committee and biannually on the progress of the cyber security strategy and uplift plan.
Section 14.1.1	Zero Trust Culture *(new section)*	N/A	Zero Trust Culture covered by: • New PSPF Requirement 0213 • Amendments to PSPF Requirements 0011, 0013 and 0098.

Location	Subject	Requirement or Table	Change
Section 15.2.1	Australian Government Hosting Certification Framework	0111	Security classified or systems of government significance information and data ~~OFFICIAL: Sensitive and PROTECTED government information and data~~ is securely hosted using a Cloud Service Provider and Data Centre Provider that has been certified against the Australian Government Hosting Certification Framework.
Section 15.3	Gateway Security *(replaces Internet Gateway Policy)*	0214	Digital Infrastructure that processes, stores or communicates Australian Government security classified information is protected by a Gateway or Security Service Edge in accordance with the Australian Government Gateway Security Standard.
Section 15.3	Gateway Security *(replaces Internet Gateway Policy)*	0113	Retired and replaced by 0214 ~~Internet-connected technology systems, and the data they process, store or communicate, are protected by a gateway in accordance with the Information Security Manual and the Gateways Policy~~
Section 15.3	Gateway Security *(replaces Internet Gateway Policy)*	0114	Gateways or Secure Service Edges that have completed an IRAP assessment (or ASD assessment for TOP SECRET gateways) against the latest version of ASD's Information Security Manual within the previous 24 months are used.
Section 15.5	Cyber Security Partnership Program *(new section)*	0215	Participate in the Australian Signals Directorate's Cyber Security Partnership Program and notify ASD in the event of a change in the entity's risk profile.
Section 15.6	Cyber Threat Intelligence Sharing Platform *(new section)*	0216	Connect to the Australian Signals Directorate's Cyber Threat Intelligence Sharing platform.
Section 15.7	Systems of Government Significance *(new section)*	0217	Declared Systems of Government Significance are protected in accordance with the Australian Government Systems of Government Significance Standard.

Personnel Domain

Location	Subject	Requirement or Table	Change
Section 17.1	Temporary Access to Resources	N/A	Temporary access to ~~SECRET information requires an existing Baseline security clearance and~~ TOP SECRET information requires an existing Negative Vetting 1 security clearance.
Section 18.6	Eligibility Waivers	0218	The Sponsoring Entity ensures clearance subjects with an eligibility waiver, or a waiver is being considered, are not given temporary or provisional access to security classified information or resources until the security vetting process is complete.

Location	Subject	Requirement or Table	Change
Section 18.6.1	Citizenship Eligibility Waivers	0149	The Accountable Authority (or the Chief Security Officer if delegated) approves a citizenship eligibility waiver ~~only~~ (after accepting the residual risk of waiving the citizenship requirement for that person and confirming that a checkable background eligibility waiver is not in place), and maintains a record of all citizenship eligibility waivers approved.
Section 18.6.2	Checkable Background Eligibility Waivers	0151	The Sponsoring Entity's Accountable Authority (or the Chief Security Officer if delegated) approves checkable background eligibility waivers ~~only~~ (after accepting the residual risk of waiving the checkable background requirement for each person and confirming that a citizenship eligibility waiver is not in place), and maintains a record of all checkable background eligibility waivers approved.
Section 19.8	Review of Decisions	Table 31	Primary review by the relevant vetting agency – an employee can seek an initial review conducted by the vetting agency. The employee has ~~120~~ 60 days from notification of the security decision to request a review under subsection 38(1) 5.24(1) of the ~~*Public Service Regulations 1999*~~ *Public Service Regulations 2023.*
Chapter 20	Australian Officials and Office Holders *(name change)*	N/A	Name change reflected throughout section.
Section 20.4	Other Commonwealth Officials *(new section)*	N/A	Introduces new policy content.

Physical Domain

Nil changes.

Contact

Protective Security Policy Section

Department of Home Affairs

PSPF Hotline (02) 5127 9999

PSPF@homeaffairs.gov.au

www.protectivesecurity.gov.au