PSPF Release 2024 (November 2024) - List of Requirements							Status	Previous PSPF (2018-October 2024) - Core and Supporting Requirements					
Req Number	Used in R24	Release 24 Requirement	Domain	Section	Applicability (All, Dept of State, security service provider, technical authority, vetting agency)	Start Date	Decision (Retain, modify, remove, replace or add)	Previous PSPF Requirement	Previous security outcome	Previous PSPF Policy	Previous Section	Previous Topic	Previous Type
1	Y	The Department of State supports portfolio entities to achieve and maintain an acceptable level of protective security through advice and guidance on government security.	GOV	01. WoAG Protective Security Roles	Departments of State	31/10/2024	Retain-Split	The accountable authority of a lead security entity must provide other entities with advice, guidance and services related to government security	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership - lead entity	Mandatory
2	Y	The Accountable Authourity complies with all Protective Security Directions.	GOV	01. WoAG Protective Security Roles	All entities	31/10/2024	Retain	The accountable authority of each entity must adhere to any direction issued by the Secretary of the Attorney-General's Department under the PSPF	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership	Mandatory
3	Y	The Technical Authority Entity provides technical advice and guidance to support entities to achieve and maintain an acceptable level of protective security.	GOV	01. WoAG Protective Security Roles	Technical Authority Entity	31/10/2024	Retain-Split	The accountable authority of a lead security entity must provide other entities with advice, guidance and services related to government security	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership - lead entity	Mandatory
4	Y	The Shared Service Provider Entity supplies security services that help relevant entities achieve and maintain an acceptable level of security	GOV	01. WoAG Protective Security Roles	Shared Service Provider Entity	31/10/2024	Retain-Split	The accountable authority of a lead security entity must ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership - lead entity	Mandatory
5	Y	The Shared Service Provider Entity develops, implements and maintains documented responsibilities and accountabilities for partnerships or security service arrangements with other entities.	GOV	01. WoAG Protective Security Roles	Shared Service Provider Entity	31/10/2024	Retain-Split	The accountable authority of a lead security entity must establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership - lead entity	Mandatory
6	Y	The Accountable Authority is answerable to their minister for the entity's protective security.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain	The accountable authority is answerable to their minister and the government for the security of their entity	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership	Mandatory
7	Y	The Accountable Authority is responsible for managing the security risks of their entity.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain	The accountable authority is answerable to their minister and the government for the security of their entity	Security Governance	01. Role of accountable authority	Core requirement and Section C.1, para 6	Protective security leadership	Mandatory
8	Y	A Chief Security Officer is appointed and empowered to oversee the entity's protective security arrangements.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain-Split	The accountable authority must appoint a Chief Security Officer (CSO) at the Senior Executive Service (note 1) level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the entity. 1. Where an entity has fewer than 100 employees the accountable authority may appoint their Chief Security Officer at the Executive Level 2 (EL2), providing the EL2: • reports directly to the accountable authority on security matters, and • has the sufficient authority and capability to perform the responsibilities of the CSO role	Security Governance	02. Management structures and responsibilities	Core requirement	Security leadership	Mandatory
9	Y	The Chief Security Officer is a Senior Executive Service officer (note 1) and holds a minimum security clearance of Negative Vetting 1. Note: 1. Where an entity has fewer than 100 employees the Accountable Authority may appoint their CSO at the EL2, providing the EL2 reports directly to the Accountable Authority on security matters, and has the sufficient authority and capability to perform the responsibilities of the CSO role.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain-Split	The accountable authority must appoint a Chief Security Officer (CSO) at the Senior Executive Service (note 1) level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the entity. 1. Where an entity has fewer than 100 employees the accountable authority may appoint their Chief Security Officer at the Executive Level 2 (EL2), providing the EL2: • reports directly to the accountable authority on security matters, and • has the sufficient authority and capability to perform the responsibilities of the CSO role	Security Governance	02. Management structures and responsibilities	Core requirement (a)	Security leadership	Mandatory
10	Y	The Chief Security Officer is accountable to the Accountable Authority for protective security matters.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	New (add)	CSO….report to the accountable authority on security matters	Security Governance	02. Management structures and responsibilities	Guidelines	CSO	Recommended
11	Y	A Chief Information Security Officer is appointed to oversee the entity's cyber security program, including information technology and operational technology.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain-Split	The Accountable authority must appoint a Chief Information Security Officer (CISO) with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity	Security Governance	02. Management structures and responsibilities	Core requirement (c)	Cyber Security leadership	Mandatory
12	Y	The Chief Information Security Officer has the appropriate capability and experience and holds a minimum security clearance of Negative Vetting 1.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain-Split	The Accountable authority must appoint a Chief Information Security Officer (CISO) with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity	Security Governance	02. Management structures and responsibilities	Core requirement (c)	Cyber Security leadership	Mandatory
13	Y	The Chief Information Security Officer is accountable to the Accountable Authority for cyber security.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	New (add)	The CISO complements the CSO role, and is also likely to report directly to the CSO or accountable authority on cyber security matters, and work with the entity's Chief Information Officer, Chief Operating Officer or other senior executives in the entity	Security Governance	02. Management structures and responsibilities	Guidelines	Management structures	Recommended
14	Y	Where appointed, security practitioners are appropriately skilled, empowered and resourced to perform their designated functions.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Modify	Effective management structures and responsibilities require people to be appropriately skilled, empowered and resourced. This is essential to achieving security outcomes.	Security Governance	02. Management structures and responsibilities	Purpose	Purpose	Mandatory
15	Y	Where appointed, security practitioners have access to training across government to maintain and upskill on new and emerging security issues.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Modify	b. empower the CSO to make decisions about: i. appointing security advisors within the entity ii. the entity's protective security planning iii. the entity's protective security practices and procedures iv. investigating, responding to, and reporting on security incidents (other than cyber incidents) 32. Under the core requirement and Requirement 1(a), the CSO is empowered to appoint security advisors and Requirement 1(b), the CISO is empowered to appoint cyber security advisors. In making these decisions, the CSO and CISO are encouraged to: determine the appropriate competencies, experience and specialist skills or qualifications required to undertake the appointed security role/s, including comprehensive knowledge of the PSPF	Security Governance	02. Management structures and responsibilities	Core requirement (b)	Appointing security advisors	Mandatory
16	Y	The Accountable Authority approves security governance arrangements that are tailored to the entity's size, complexity and risk environment.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Modify	14. Requirement 1 states that the CSO is responsible for directing all areas of security to protect people, information and assets. This includes tailoring security arrangements to the scale and complexity of the entity. The intention is that as a single senior officer with central oversight and responsibility for security arrangements (other than for cyber security) in the entity, they have the flexibility to delegate the day-to-day activities of protective security where required.	Security Governance	02. Management structures and responsibilities	Requirement 1 - implied	CSO Responsibilities	Passive control
17	Y	A dedicated security email address is established and monitored as the central conduit for distribution of protective security-related information across the entity.	GOV	02. Entity Protective Security Roles and Responsibilitities	All entities	31/10/2024	Retain	Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.	Security Governance	02. Management structures and responsibilities	Supporting requirement 5	General email	Mandatory
18	Y	A security plan is developed, implemented and maintained to address the mandatory elements of the plan.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain-Split	Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks.	Security Governance	03. Security planning and risk management	Core requirement	Security plan	Mandatory
19	Y	The Accountable Authority approves the entity's security plan.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain-Split	Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks.	Security Governance	03. Security planning and risk management	Core requirement	Security plan	Mandatory
20	Y	The security plan is considered annually and reviewed at least every two years to confirm its adequacy and ability to adapt to shifts in the entity's risk, threat or operating environment.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	The security plan (and supporting security plans) must be reviewed at least every two years. The review process must include how the entity will: a. determine the adequacy of existing measures and mitigation controls, b. respond to and manage significant shifts in the entity's risk, threat and operating environment.	Security Governance	03. Security planning and risk management	Supporting requirement 1	Security plan	Mandatory

21	Y	Procedures are developed, implemented and maintained to ensure all elements of the entity's security plan are achieved.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain-Split	Entities must develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported c. relevant security policy or legislative obligations are met.	Security Governance	02. Management structures and responsibilities	Supporting requirement 2 (a)	Security procedures	Mandatory
22	Y	Develop, establish and implement security monitoring arrangements to identify the effectiveness of the entity's security plan and establish a continuous cycle of improvement.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Modify	Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.	Security Governance	04. Security maturity monitoring	Core requirement	Monitoring	Mandatory
23	Y	The Accountable Authority and Chief Security Officer develops, implements and maintains a program to foster a positive security culture in the entity and support the secure delivery of government business.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Modify-Split	The accountable authority must ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.	Security Governance	02. Management structures and responsibilities	Core requirement (e)	Security leadership	Mandatory
24	Y	Security awareness training is provided to personnel, including contractors, at engagement and annually thereafter.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Entities must provide all personnel, including contractors, with security awareness training at engagement and annually thereafter	Security Governance	02. Management structures and responsibilities	Supporting requirement 3	Security training	Mandatory
25	Y	Targeted security training is provided to personnel, including contractors, in specialist or high-risk positions.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.	Security Governance	02. Management structures and responsibilities	Supporting requirement 4	Specific training	Mandatory
26	Y	Procedures are developed, implemented and maintained to ensure security incidents are managed and responded to.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain-Split	Entities must develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported c. relevant security policy or legislative obligations are met.	Security Governance	02. Management structures and responsibilities	Supporting requirement 2 (b)	Security procedures	Mandatory
27	Y	Security incident management and response plans are incorporated into the entity's business continuity arrangements.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
28	Y	Significant or externally reportable security incidents and referral obligations are reported to the relevant authority (or authorities) within the applicable timeframe.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Each entity must report any significant or reportable security incidents at the time they occur to: a. the relevant authority (as detailed in Table 3) b. other affected entities, and c. the Department of Home Affairs.	Security Governance	05. Reporting on security	Supporting requirement 2	Reporting security incidents	Mandatory
29	Y	Procedures are developed, implemented and maintained to investigate security incidents in accordance with the principles of the Australian Government Investigations Standards.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain-Split	Entities must develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported c. relevant security policy or legislative obligations are met.	Security Governance	02. Management structures and responsibilities	Supporting requirement 2	Security procedures	Mandatory
30	Y	The principles of procedural fairness are applied to all security investigations, with due regard to national security considerations.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	New (add)	76. The principles of procedural fairness apply to all investigations	Security Governance		Para 76	Security investigations	Passive control
31	Y	The annual protective security report is provided to the entity's Minister.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain-Split	Each entity must report on security each financial year to its portfolio minister and the Department of Home Affairs addressing whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF.	Security Governance	05. Reporting on security	Core requirement (ai)	Reporting	Mandatory
32	Y	The annual protective security report is submitted to the Department of Home Affairs.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain-Split	Each entity must report on security each financial year to its portfolio minister and the Department of Home Affairs addressing whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF.	Security Governance	05. Reporting on security	Core requirement (ai)	Reporting	Mandatory
33	Y	The Accountable Authority approves the entity's annual protective security report and confirms that they have verified the report's content.	GOV	04. Protective Security Reporting	All entities	31/10/2024	New (add)						
34	Y	Entities cooperate with the Department of Home Affairs' assurance activities to review annual protective security reports.	GOV	04. Protective Security Reporting	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
35	Y	The annual Cyber Security Survey is submitted to the Australian Signals Directorate.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Each entity must report on security to the Australian Signals Directorate in relation to cyber security matters.	Security Governance	05. Reporting on security	Supporting Requirement 3	ASD cyber security survey	Mandatory
36	Y	The Accountable Authority determines their entity's tolerance for security risks and documents in the security plan.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	The accountable authority of each entity must determine their entity's tolerance for security risks	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership	Mandatory
37	Y	A risk steward (or manager) is identified and responsible for each security risk or category of security risk, including for shared risks.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	Entities must identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.	Security Governance	03. Security planning and risk management	Supporting requirement 3	Risk steward	Mandatory
38	Y	The Accountable Authority considers the impact that their security risk management decisions could potentially have on other entities, and shares information on risks where appropriate.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	The accountable authority of each entity must consider the implications their risk management decisions have for other entities, and share information on risks where appropriate	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership	Mandatory
39	Y	The entity is accountable for the management of security risks arising from procuring goods and services and ensures procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Modify-Split	Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements	Security Governance	06. Security governance for contracted goods and service providers	Core requirement	Procurement security risks	Mandatory
40	Y	Procurement, contracts and third-party outsourced arrangements, contain proportionate security terms and conditions to ensure service providers, contractors and subcontractors comply with relevant PSPF Requirements and avoid exposing the entity or the Australian Government to an unacceptable level of risk.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	When procuring goods or services, entities must put in place proportionate protective security measures by identifying and documenting: a. specific security risks to its people, information and assets, and b. mitigations for identified risks.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 1	Assessing and managing security risks of procurement	Mandatory
41	Y	Entity ensures service providers, contractors and subcontractors comply with relevant PSPF Requirements as detailed by the entity.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain-Split	Entities must ensure that contracts for goods and services include relevant security terms and conditions for the provider to apply appropriate information, physical and personnel security requirements of the PSPF. Also, second part of core requirement: Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements	Security Governance	06. Security governance for contracted goods and service providers	Core requirement + Supporting Requirement 2	Establishing protective security terms and conditions in contracts	Mandatory
42	Y	Contractual security terms and conditions require service providers to report any actual or suspected security incidents to the entity, and follow reasonable direction from the entity arising from incident investigations.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain-Split	Entities must ensure that contracts for goods and services include relevant security terms and conditions for the provider to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement, and c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 2	Establishing protective security terms and conditions in contracts	Mandatory
43	Y	Government entities providing outsourced services provide IRAP assessment reports to the government entities consuming, or looking to consume, their services.	RISK	06. Third Party Risk Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
44	Y	Contract security terms and conditions are monitored and reviewed to ensure the specified security controls, terms and conditions are implemented, operated and maintained by the contracted provider, including any subcontractors, over the life of a contract.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain-Split	When managing contracts, entities must put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and b. manage any changes to the provision of goods or services, and reassess security risks.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 3	Ongoing management of protective security in contracts	Mandatory
45	Y	Contractual terms and conditions include appropriate security arrangements for the completion or termination of the contract	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Entities must implement appropriate security arrangements at completion or termination of a contract.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 4	Completion or termination of a contract	Mandatory

46	Y	Procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence risks.	RISK	06. Third Party Risk Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
47	Y	Security risks arising from contractual arrangements for the provision of goods and services are managed, reassessed and adjusted over the life of a contract.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain-Split	When managing contracts, entities must put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and b. manage any changes to the provision of goods or services, and reassess security risks.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 3	Ongoing management of protective security in contracts	Mandatory
48	Y	Secure and verifiable third-party vendors, providers, partners and associated services are used unless business operations require use, and the residual risks are managed and approved by the Chief Information Security Officer.	RISK	06. Third Party Risk Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
49	Y	Entities manage the security risks associated with engaging with foreign partners.	RISK	06. Third Party Risk Management	All entities	31/10/2024	New (add)						
50	Y	Personnel do not publicise their security clearance level on social media platforms, including employment-focused platforms such as LinkedIn.	RISK	07. Countering Foreign Interference and Espionage	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
51	Y	An insider threat program is implemented by entities that manage Baseline to Positive Vetting security clearance subjects to manage the risk of insider threat in the entity.	RISK	07. Countering Foreign Interference and Espionage	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
52	Y	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement or standard, the Accountable Authority may vary application, for a limited period of time, consistent with the entity's risk tolerance.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain-Split	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority may vary application, for a limited period of time, consistent with the entity's risk tolerance. If used, the accountable authority must record the decision to vary in the annual report on security and advise remedial action taken to reduce the risk to the entity.	Security Governance	01. Role of accountable authority	Supporting requirement 1 (a)	Exceptional circumstances	Mandatory
53	Y	Decisions to vary implementation of a PSPF requirement or standard due to exceptional circumstances are documented in the entity's security plan.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain-Split	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority may vary application, for a limited period of time, consistent with the entity's risk tolerance. If used, the accountable authority must record the decision to vary in the annual report on security and advise remedial action taken to reduce the risk to the entity.	Security Governance	01. Role of accountable authority	Supporting requirement 1 (b)	Exceptional circumstances	Mandatory
54	Y	Decisions to implement an alternative mitigation measure that meets or exceeds a PSPF requirement or standard are reviewed and reported annually.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they must document the decision and adjust the maturity level for the related PSPF requirement.	Security Governance	03. Security planning and risk management	Supporting requirement 6	Alternative mitigations	Mandatory
55	Y	A business continuity plan is developed, implemented and maintained to respond effectively and minimise the impacts of significant business disruptions to the entity's critical services and assets, and other services and assets when warranted by a threat and security risk assessment.	RISK	08. Contingency Planning	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
56	Y	Plans for managing a broad range of emergencies are integrated within the business continuity plan.	RISK	08. Contingency Planning	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
57	Y	Personnel who are likely to be impacted are notified if there is a heightened risk of an emergency.	RISK	08. Contingency Planning	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
58	Y	The originator remains responsible for controlling the sanitisation, reclassification or declassification of official and security classified information, and approves any changes to the information's security classification.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	The originator must remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity must not remove or change information's classification without the originator's approval.	Information Security	08. Classification System	Supporting Requirement 3	Declassification	Mandatory
59	Y	The value, importance or sensitivity of official information (intended for use as an official record) is assessed by the originator by considering the potential damage to the government, the national interest, organisations or individuals that would arise if the information's confidentiality were compromised.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	The originator must determine whether information being generated is official information (intended for use as an official record) and whether that information is security classified.	Information Security	08. Classification System	Supporting Requirement 1	Identifying information holdings	Mandatory
60	Y	The security classification is set at the lowest reasonable level.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain-Split	To decide which security classification to apply, the originator must: ii. set the security classification at the lowest reasonable level.	Information Security	08. Classification System	Supporting Requirement 2 (ii)	Assessing security classified information	Mandatory
61	Y	Security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain-Split	The originator must clearly identify security classified information, including emails, using applicable protective markings by: a. using text-based protective markings to mark security classified information (and associated metadata), unless impractical for operational reasons	Information Security	08. Classification System	Supporting Requirement 4 (a)	Marking information	Mandatory
62	Y	The minimum protections and handling requirements are applied to protect OFFICIAL and security classified information.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	Entities must ensure OFFICIAL and security classified information is used, stored, carried and travelled with securely in accordance with the minimum protection requirements set out in Annexes A to C.	Information Security	08. Classification System	Supporting Requirement 7 (a)	Minimum protections and handling requirements	Mandatory
63	Y	The Australian Government Security Caveat Standard and special handling requirements imposed by the controlling authority are applied to protect security caveated information.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	For all caveated information, entities must apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.	Information Security	08. Classification System	Supporting Requirement 6 (c)	Caveats and accountable material	Mandatory
64	Y	Security caveats are clearly marked as text and only appear in conjunction with a security classification of PROTECTED or higher.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	Caveats must be marked as text and (with the exception of the NATIONAL CABINET caveat) only appear in conjunction with a security classification of PROTECTD or higher. The NATIONAL CABINET caveat can appear in conjunction with a security classification of OFFICIAL: Sensitive marking or higher.	Information Security	08. Classification System	Supporting Requirement 6 (a)	Caveats and accountable material	Mandatory
65	Y	Accountable material has page and reference numbering.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	Entities must ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements.	Information Security	08. Classification System	Supporting Requirement 6 (b)	Caveats and accountable material	Mandatory
66	Y	Accountable material is handled in accordance with any special handling requirements imposed by the originator and security caveat owner detailed in the Australian Government Security Caveat Standard.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	For all caveated information, entities must apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.					
67	Y	The Australian Government Email Protective Marking Standard is applied to protect OFFICIAL and security classified information exchanged by email in and between Australian Government entities, including other authorised parties.	INFO	09. Classifications & Caveats	All entitiies	31/10/2024	Retain	The originator must clearly identify security classified information, including emails, by using applicable protective markings.	Information Security	08. Classification System	Supporting requirement 4	Marking information	Mandatory
68	Y	The Australian Government Recordkeeping Metadata Standard's 'Security Classification' property (and where relevant, the 'Security Caveat' property) is applied to protectively mark information on technology systems that store, process or communicate security classified information.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain-Split	Entities must apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate security classified information: a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property)	Information Security	08. Classification System	Supporting Requirement 5 (a)	Using metadata to mark information	Mandatory
69	Y	Apply the Australian Government Recordkeeping Metadata Standard's 'Rights' property where the entity wishes to categorise information content by the type of restrictions on access.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain-Split	Entities must apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate security classified information: b. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.	Information Security	08. Classification System	Supporting Requirement 5 (b)	Using metadata to mark information	Mandatory

70	Y	Security classified discussions and dissemination of security classified information are only held in approved locations.	INFO	09. Classifications & Caveats	All entities	31/10/2024	Retain	Entities must ensure security classified discussions are only held in approved locations as set out in Annex D.	Information Security	08. Classification System	Supporting Requirement 9	Security classified discussions	Mandatory
71	Y	Entity implements operational controls for its information holdings that are proportional to their value, importance and sensitivity.	INFO	10. Information Holdings	All entities	31/10/2024	Retain-Split	Each entity must: iii. implement operational controls for these information holdings proportional to their value, importance and sensitivity.	Information Security	08. Classification System	Core requirement (iii)	Information holdings	Mandatory
72	Y	An auditable register is maintained for TOP SECRET information and accountable material.	INFO	10. Information Holdings	All entities	31/10/2024	Retain-Split	Entities must ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements.					
73	Y	OFFICIAL and security classified information is disposed of securely in accordance with the Minimum Protections and Handling Requirements, Information Security Manual, the Records Authorities, a Normal Administrative Practice and the *Archives Act 1983* .	INFO	11. Information Disposal	All entities	31/10/2024	Retain-Split	Entities must ensure OFFICIAL and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to C. This includes ensuring security classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.	Information Security	08. Classification System	Supporting Requirement 8	Disposal	Mandatory
74	Y	Security classified information is appropriately destroyed in accordance with the Minimum Protections and Handling Requirements when it has passed the minimum retention requirements or reaches authorised destruction dates.	INFO	11. Information Disposal	All entities	31/10/2024	Retain-Split	Entities must ensure OFFICIAL and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to C. This includes ensuring security classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.	Information Security	08. Classification System	Supporting Requirement 8	Disposal	Mandatory
75	Y	Access to security classified information or resources is only provided to people outside the entity with the appropriate security clearance (where required) and a need-to-know, and is transferred in accordance with the Minimum Protections and Handling Requirements.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	To reduce the risk of unauthorised disclosure, entities must ensure access to security classified information or resources is only provided to people with a need-to-know.	Information Security	09. Access to information	Supporting Requirement 2	Limiting access to security classified information and resources	Mandatory
76	Y	The Memorandum of Understanding between the Commonwealth, States and Territories is applied when sharing information with state and territory government agencies.	INFO	12. Information Sharing	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
77	Y	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.	INFO	12. Information Sharing	All entities	31/10/2024	Modify	When disclosing security classified information or resources to a person or organisation outside of government, entities must have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.	Information Security	09. Access to information	Supporting Requirement 1	Formalised agreements for sharing information and resources	Mandatory
78	Y	Provisions are met concerning the security of people, information and resources contained in international agreements and arrangements to which Australia is a party.	INFO	12. Information sharing	All entities	31/10/2024	Retain	Each entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.	Security Governance	07. Security governance for international sharing	Core requirement	International sharing and agreements	Mandatory
79	Y	Australian Government security classified information or resources shared with a foreign entity is protected by an explicit legislative provision, international agreement or international arrangement.	INFO	12. Information sharing	All entities	31/10/2024	Retain	When an entity shares security classified Australian Government information or assets with a foreign entity there must be an explicit legislative provision, an international agreement or an international arrangement in place for its protection.	Security Governance	07. Security governance for international sharing	Supporting requirement 1(a)	Sharing information with a foreign entity	Mandatory
80	Y	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.	INFO	12. Information sharing	All entities	31/10/2024	Retain	The following limitation applies, even when an international agreement or international arrangement is in place: i. entities must not share Australian Government information bearing the Australian Eyes Only (AUSTEO) caveat with a person who is not an Australian citizen.	Security Governance	07. Security governance for international sharing	Supporting requirement 1(bi)	Sharing information with a foreign entity	Mandatory
81	Y	Australian Government classified information or resources bearing the Australian Government Access Only (AGAO) caveat is not shared with a person who is not an Australia citizen, even when an international agreement or international arrangement is in place, unless they are working for, or seconded to, an entity that is a member of National Intelligence Community, the Department of Defence or the Australian Submarine Agency.	INFO	12. Information sharing	All entities	31/10/2024	retain	The following limitation applies, even when an international agreement or international arrangement is in place: ii. entities, other than members of the National Intelligence Community or the Department of Defence must not share Australian Government information bearing the Australian Government Access Only (AGAO) caveat with a person who is not an Australian citizen.	Security Governance	07. Security governance for international sharing	Supporting requirement 1(bii)	Sharing information with a foreign entity	Mandatory
82	Y	Where an international agreement or international arrangement is in place, security classified foreign entity information or resources are safeguarded in accordance with the provisions set out in the agreement or arrangement.	INFO	12. Information sharing	All entities	31/10/2024	retain	Where an international agreement or international arrangement is in place, entities must safeguard security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement.	Security Governance	07. Security governance for international sharing	Supporting requirement 2	Safeguarding foreign information	Mandatory
83	Y	Australian Government security classified information or resources shared with a foreign non-government stakeholder is protected by an explicit legislative provision, international agreement or international arrangement.	INFO	12. Information sharing	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
84	Y	The Australian Signals Directorate's Information Security Manual cyber security principles are applied during all stages of the lifecycle of each system.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Modify-Split	Each entity must ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual's cyber security principles during all stages of the lifecycle of each system.	Information Security	11. Robust ICT systems	Core requirement	Safeguard systems	Mandatory
85	Y	The Australian Signals Directorate's Information Security Manual controls and cyber security guidelines are applied on a risk-based approach.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Modify-Split	Each entity must ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual's cyber security principles during all stages of the lifecycle of each system.	Information Security	11. Robust ICT systems	Core requirement	Safeguard systems	Mandatory
86	Y	The Authorising Officer authorises each technology system to operate based on the acceptance of the residual security risks associated with its operation before that system process, store or communicate government information or data.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain-Split	Entities must only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.	Information Security	11. Robust ICT systems	Supporting Requirement 1	Authorisation of ICT systems to operate	Mandatory
87	Y	Decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system are based on the Information Security Manual's risk-based approach to cyber security.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain-Split	When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate must be based on the Information Security Manual's six step risk-based approach for cyber security.	Information Security	11. Robust ICT systems	Supporting Requirement 1	Authorisation of ICT systems to operate	Mandatory
88	Y	The technology system is authorised to the highest security classification of the information and data it will process, store or communication.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
89	Y	A register of the entity's authorised technology systems is developed, implemented and maintained and includes the name and position of the Authorising Officer, system owner, date of authorisation, and any decisions to accept residual security risks.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
90	Y	Each technology system's suitability to be authorised to operate is reassessed when it undergoes significant functionality or architectural change, or where the system's security environment has changed considerably.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
91	Y	The TikTok application is prevented from being installed, and existing instances are removed, on government devices, unless a legitimate business reason exists which necessitates the installation or ongoing presence of the application.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	Direction 01/2023	Direction	Direction 01/2023	Direction 01/2023	TikTok Application	Mandatory

92	Y	The Chief Security Officer or Chief Information Security Officer approves any legitimate business reason for the use of the TikTok application on government devices and ensures the following mitigations are in place to manage security risks: • Ensure the TikTok application is installed and accessed only on a separate, standalone device without access to services that process or access official and classified information. • Ensure the separate, standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information. • Ensure metadata has been removed from photos, videos and documents when uploading any content to TikTok. • Minimise, where possible, the sharing of personal identifying content on the TikTok application. • Use an official generic email address (for example, a group mailbox) for each TikTok account. • Use multi-factor authentication and unique passphrases for each TikTok account. • Ensure that devices that access the TikTok application are using the latest available operating system in order to control individual mobile application permissions. Regularly check for and update the application to ensure the latest version is used. • Only install the TikTok application from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store. • Ensure only authorised users have access to corporate TikTok accounts and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access. • Carefully and regularly review the terms and conditions, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required. • Delete the TikTok application from devices when access is no longer needed.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	Direction 01/2023	Direction	Direction 01/2023	Direction 01/2023	TikTok Application	Mandatory
93	Y	The Australian Signals Directorate's temporary mitigations for legacy IT are applied to manage legacy information technology that cannot yet be replaced.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
94	Y	Technology assets and their components, classified as SECRET or below are stored in the appropriate Security Zone based on their aggregated security classification or business impact level.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Entities must certify and accredit the security zone for ICT security classified information with an extreme business impact level.	Physical Security	16. Entity facilities	Requirement 9 (a)	ICT facilities	Mandatory
95	Y	Technology assets and their components classified as TOP SECRET are stored in suitable SCEC-endorsed racks or compartments within an accredited Security Zone Five area meeting ASIO Technical Note 5/12 – Compartments within Zone Five areas requirements.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Entities must ensure that all TOP SECRET information ICT facilities are in compartments within an accredited Zone Five area and comply with Annex A – ASIO Technical Note 5/12 – Compartments within Zone Five areas.	Physical Security	16. Entity facilities	Requirement 9 (b)	ICT facilities	Mandatory
96	Y	Outsourced facilities that house technology assets and their components with a catastrophic business impact level are certified by ASIO-T4 physical security and accredited by ASD before they are used operationally.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Entities must before using outsourced ICT facilities operationally obtain ASIO-T4 physical security certification for the outsourced ICT facility to hold information that, if compromised, would have a catastrophic business impact level.	Physical Security	16. Entity facilities	Requirement 9 (c)	ICT facilities	Mandatory
97	Y	Technology assets are disposed of securely in accordance with the Information Security Manual.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Entities must dispose of physical assets securely.	Physical Security	15. Physical security for entity resources	Supporting requirement 3	Disposal	Mandatory
98	Y	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.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
99	Y	Patch applications mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: ii. patch applications	Information Security	10. Safeguarding data from cyber threats	Core requirement (aii)	Cyber mitigations strategies	Mandatory
100	Y	Patch operating systems mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: vi. patch operating systems	Information Security	10. Safeguarding data from cyber threats	Core requirement (avi)	Cyber mitigations strategies	Mandatory
101	Y	Multi-factor authentication mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	a. Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: vii. multi-factor authentication	Information Security	10. Safeguarding data from cyber threats	Core requirement (avii)	Cyber mitigations strategies	Mandatory
102	Y	Restrict administrative privileges mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: v. restrict administrative privileges	Information Security	10. Safeguarding data from cyber threats	Core requirement (av)	Cyber mitigations strategies	Mandatory
103	Y	Application control mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: i. application control	Information Security	10. Safeguarding data from cyber threats	Core requirement (ai)	Cyber mitigations strategies	Mandatory
104	Y	Restrict Microsoft Office macros mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: iii. configure Microsoft Office macro settings	Information Security	10. Safeguarding data from cyber threats	Core requirement (aiii)	Cyber mitigations strategies	Mandatory
105	Y	User application hardening mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: iv. user application hardening	Information Security	10. Safeguarding data from cyber threats	Core requirement (aiv)	Cyber mitigations strategies	Mandatory
106	Y	Regular back-ups mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain-Split	Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the Strategies to Mitigate Cyber Security Incidents: viii. regular backups	Information Security	10. Safeguarding data from cyber threats	Core requirement (aviii)	Cyber mitigations strategies	Mandatory
107	Y	The remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents are considered and, where required, implemented to achieve an acceptable level of residual risk for their entity.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Each entity must mitigate common cyber threats by considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents need to be implemented to achieve an acceptable level of residual risk for their entity.	Information Security	10. Safeguarding data from cyber threats	Core requirement (b)	Cyber mitigations strategies	Mandatory
108	Y	A Protective Domain Name System service or other security mechanisms is used to prevent connections to and from known malicious endpoints..	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Entities must implement security controls that prevent connections to or from known malicious endpoints, through the use of a Protective Domain Name System (PDNS) service or other security mechanisms.	Information Security	11. Robust ICT systems	Supporting Requirement 3	Prevent connections to or from known malicious endpoints	Mandatory
109	Y	Cloud Service Providers that have completed an IRAP assessment against the current version of ASD's Information Security Manual within the previous 24 months are used.	TECH	15. Cyber Security Programs	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
110	Y	Entities consider IRAP assessment recommendations and findings and implement on a risk-based approach.	TECH	15. Cyber Security Programs	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
111	Y	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.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Entities must ensure the secure hosting of security classified government information and data through the use of certified services and associated infrastructure by applying the Hosting Certification Framework (HCF).	Information Security	11. Robust ICT systems	Supporting Requirement 4	Hosting Certification Framework	Mandatory
112	Y	The Data Centre Facilities Supplies Panel is used when procuring certified data centre space and services.	TECH	15. Cyber Security Programs	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A

113	Y	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.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Entities must protect internet-connected ICT systems, and the information and data they process, store or communicate, by implementing a gateway consistent with the Information Security Manual and the Gateways Policy.	Information Security	11. Robust ICT systems	Supporting Requirement 2	Gateways	Mandatory
114	Y	Gateways that have completed an IRAP assessment against ASD's Information Security Manual within the previous 24 months are used.	TECH	15. Cyber Security Programs	All entities	31/10/2024	New (add)	N/A new control	N/A	N/A	N/A	N/A	N/A
115	Y	A vulnerability disclosure program and supporting processes and procedures are established to receive, verify, resolve and report on vulnerabilities disclosed by both internal and external sources.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Modify	Entities must have in place a vulnerability disclosure program.	Information Security	11. Robust ICT systems	Supporting Requirement 5	Vulnerability Disclosure Program	Mandatory
116	Y	The eligibility and suitability of personnel who have access to Australian Government people, information and resources is ensured.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Retain	Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).	Personnel Security	12. Eligibility and suitability of personnel	Core requirement	Eligibility and suitability of personnel	Mandatory
117	Y	The pre-employment screening identity check is conducted for all personnel, to verify identity to at least Level 3 (High) of Assurance of the National Identity Proofing Guidelines.	PER	16. Pre-Employment Eligibility	All entities (Note: does not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984	31/10/2024	Modify	Entities must undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm. **Requirement 1** applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources (*Note 1*). Requirements 2 and 3 apply to security cleared personnel only. *Note 1. Requirements 1 and 2c do not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984. For further information, see Annex A of*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 1	Pre-employment screening	Mandatory
118	Y	Biographic information in identity documents is verified to ensure the information matches the original record	PER	16. Pre-Employment Eligibility	All entities (Note: does not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984	31/10/2024	Modify	Entities must undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm. **Requirement 1** applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources (*Note 1*). Requirements 2 and 3 apply to security cleared personnel only. *Note 1. Requirements 1 and 2c do not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984. For further information, see Annex A of*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 1(a)	Pre-employment screening	Mandatory
119	Y	The pre-employment screening eligibility check is conducted for all personnel, to confirm their eligibility to work in Australia and for the Australian Government.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Modify	Entities must undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm. **Requirement 1** applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources (*Note 1*). Requirements 2 and 3 apply to security cleared personnel only. *Note 1. Requirements 1 and 2c do not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984. For further information, see Annex A of*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 1(b)	Pre-employment screening	Mandatory
120	Y	The entity obtains assurance of each 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, during pre-employment screening.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Modify	Entities must undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm. **Requirement 1** applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources (*Note 1*). Requirements 2 and 3 apply to security cleared personnel only. *Note 1. Requirements 1 and 2c do not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984. For further information, see Annex A of*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 1(c)	Pre-employment screening	Mandatory
121	Y	Prior to granting temporary access to security classified information or resources, pre-employment checks are completed, and an existing Negative Vetting 1 security clearance is confirmed prior to granting temporary access to TOP SECRET information data or resources.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance, and	Information Security	09. Access to information	Supporting Requirement 4 (b & d)	Temporary access to security classified information and resources	Mandatory

122	Y	A risk assessment determines whether a person is granted temporary access to security classified information or resources.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person, or ii. up to a maximum of three months in a 12-month period b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) c. supervise all temporary access d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance, and e. deny temporary access to classified caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).	Information Security	09. Access to information	Supporting Requirement 4	Temporary access to security classified information and resources	Mandatory
123	Y	Temporary access to security classified information, resources and activities is supervised.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: c. supervise all temporary access	Information Security	09. Access to information	Supporting Requirement 4 (c)	Temporary access to security classified information and resources	Mandatory
124	Y	Short-term temporary access to security classified information, resources and activities is limited to the period in which an application for a security clearance is being processed for the particular person, or up to a total combined maximum of three months in a 12-month period for all entities. *Note: 12-months refers to the preceding 12-months from the date the short-term access would be granted.*	PER	17. Access to Resources	All entities	31/10/2024	Retain	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person, or ii. up to a maximum of three months in a 12-month period	Information Security	09. Access to information	Supporting Requirement 4 (a)	Temporary access to security classified information and resources	Mandatory
125	Y	The Authorised Vetting Agency confirms that the completed security clearance pack has been received and that no initial concerns have been identified for the clearance subject, before short-term temporary access is changed to provisional temporary access.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	22. The type of temporary access can be changed from short-term to provisional once the vetting agency has confirmed that the completed security clearance pack has been received and advises the entity that no initial concerns have been identified.	Information Security	09. Access to information	Para 22	Temporary access to security classified information and resources	Passive control
126	Y	Temporary access to classified caveated information, resources or activities is not granted, other than in exceptional circumstances, and only with the approval of the caveat controlling authority.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities must: e. deny temporary access to classified caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).	Information Security	09. Access to information	Supporting Requirement 4 (e)	Temporary access to security classified information and resources	Mandatory
127	Y	Prior to granting temporary access, the entity obtains an undertaking from the person to protect the security classified information, resources and activities they will access.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	26. The Department of Home Affairs considers there is merit in obtaining an undertaking (e.g. through a confidentiality or non-disclosure agreement) from the person to protect official information.	Information Security	09. Access to information	Paragraph 26	Temporary access to security classified resources	Recommended
128	Y	Prior to granting temporary access, the entity obtains agreement from any other entity (or third party) whose security classified information, resources and activities will be accessed by the person during the temporary access period.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	25. Where an entity intends to grant temporary access to classified information from another entity or third party, the Department of Home Affairs recommends consulting the other entity or party, where appropriate, and obtaining agreement for temporary access to their classified information.	Information Security	09. Access to information	Paragraph 25	Temporary access to security classified resources	Recommended
129	Y	Access to official information is facilitated for entity personnel and other relevant stakeholders.	PER	17. Access to Resources	All entities	31/10/2024	Retain-Split	Each entity must enable appropriate access to official information. This includes: a. sharing information within the entity, as well as with other relevant stakeholders	Information Security	09. Access to information	Core requirement (a)	Appropriate access to information	Mandatory
130	Y	Appropriate access to official information is enabled, including controlling access (including remote access) to supporting technology systems, networks, infrastructure, devices and applications.	PER	17. Access to Resources	All entities	31/10/2024	Retain-Split	Each entity must enable appropriate access to official information. This includes: c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.	Information Security	09. Access to information	Core requirement (c)	Appropriate access to information	Mandatory
131	Y	Access to security classified information or resources is only given to entity personnel with a need-to-know that information.	PER	17. Access to Resources	All entities	31/10/2024	Retain-Split	Each entity must enable appropriate access to official information. This includes: a. sharing information within the entity, as well as with other relevant stakeholders b. ensuring that those who access security classified information have an appropriate security clearance and need to know that information, and c. controlling access (including remote access) to supporting ICT systems, networks, infrastructure, devices and applications.	Information Security	09. Access to information	Core requirement (b)	Appropriate access to information	Mandatory
132	Y	Personnel requiring ongoing access to security classified information or resources are security cleared to the appropriate level.	PER	17. Access to Resources	All entities	31/10/2024	Retain-Split	Entities must ensure that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level (as per table on ***'policy 9 table'*** tab). Noting that some Australian office holders are not required to hold a security clearance.	Information Security	09. Access to information	Supporting Requirement 3 (a)	Ongoing access security classified information and resources	Mandatory
133	Y	Personnel requiring access to caveated information meet any clearance and suitability requirements imposed by the originator and caveat controlling authority.	PER	17. Access to Resources	All entities	31/10/2024	Retain-Split	Entities must ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.	Information Security	09. Access to information	Supporting Requirement 3 (b)	Ongoing access security classified information and resources	Mandatory
134	Y	A unique user identification, authentication and authorisation practice is implemented on each occasion where system access is granted, to manage access to systems holding security classified information.	PER	17. Access to Resources	All entities	31/10/2024	Retain	To manage access to information systems holding security classified information, entities must implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.	Information Security	09. Access to information	Supporting Requirement 5	Managing access to information systems	Mandatory
135	Y	A security risk assessment of the proposed location and work environment informs decisions by the Chief Security Officer to allow personnel to work in another government entity's facilities in Australia..	PER	17. Access to Resources	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
136	Y	An agreement is in place to manage the security risks associated with personnel working in another government entity's facilities in Australia.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
137	Y	Approval for remote access to TOP SECRET information, data or systems in international locations outside of facilities meeting PSPF requirements, is only granted if approved by the Australian Signals Directorate.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
138	Y	A security risk assessment of the proposed location and work environment informs decisions to allow personnel to work remotely in international locations.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
139	Y	Personnel are not granted approval to work remotely in locations where Australian Government information, or resources are exposed to extrajudicial directions from a foreign government that conflict with Australian law, unless operationally required, and the residual risks are managed and approved by the Chief Security Officer.	PER	17. Access to Resources	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A

140	Y	The Australian Government Security Vetting Agency (AGSVA) or the TOP SECRET-Privileged Access Vetting Authority is used to conduct security vetting, or where authorised, the entity conducts security vetting in a manner consistent with the Personnel Security Vetting Process and Australian Government Personnel Security Adjudicative Standard.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	Entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.	Personnel Security	12. Eligibility and suitability of personnel	Core requirement	Authorised vetting providers	Mandatory
141	Y	All vetting personnel attain and maintain the required skills and competencies for their role.	PER	18. Security Clearances	Authorised Vetting Agency	31/10/2024	Modify	Authorised vetting agencies must ensure all vetting personnel attain and maintain the required skills and competencies for their role.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(h)	Personnel security vetting standards	Mandatory
142	Y	The gaining sponsoring entity establishes new clearance conditions before assuming sponsorship of an existing security clearance that is subject to clearance conditions.	PER	18. Security Clearances	All entities	31/10/2024	Modify	If a clearance is subject to an eligibility waiver or clearance conditions, the vetting agency will advise the gaining sponsoring entity. For clearances subject to an eligibility waiver, the gaining sponsoring entity will accept and undertake the exceptional business requirement and risk assessment provisions in accordance with Requirements 2d and 2e, prior to requesting transfer of sponsorship. For clearances subject to clearance conditions, the gaining sponsoring entity will need to accept the clearance conditions.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2 (d and e)	Recognition of existing clearances	Passive control
143	y	The gaining sponsoring entity undertakes the exceptional business requirement and risk assessment provisions prior to requesting transfer of sponsorship of an existing security clearance that is subject to an eligibility waiver.	PER	18. Security Clearances	All entities	31/10/2024	Modify	If a clearance is subject to an eligibility waiver or clearance conditions, the vetting agency will advise the gaining sponsoring entity. For clearances subject to an eligibility waiver, the gaining sponsoring entity will accept and undertake the exceptional business requirement and risk assessment provisions in accordance with Requirements 2d and 2e, prior to requesting transfer of sponsorship. For clearances subject to clearance conditions, the gaining sponsoring entity will need to accept the clearance conditions.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2 (d and e)	Recognition of existing clearances	Passive control
144	Y	The Authorised Vetting Agency only issues a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government.	PER	18. Security Clearances	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must only issue a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(a)	Personnel security vetting standards	Mandatory
145	Y	Positions that require a security clearance are identified and the level of clearance required is documented.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	Entities must identify and record positions that require a security clearance and the level of clearance required.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(a)	Security clearances	Mandatory
146	Y	Each person working in an identified position has a valid security clearance issued by the relevant Authorised Vetting Agency.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	Entities must ensure each person working in an identified position has a valid security clearance issued by an authorised vetting agency.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(b)	Security clearances	Mandatory
147	Y	Australian citizenship is confirmed and pre-employment screening is completed before the entity seeks a security clearance for a person in a position identified as requiring a security clearance.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	Entities must, before seeking a security clearance, confirm that the person meets pre-employment screening requirements (*Note i*) and is an Australian citizen. *Note i: An exception applies for entities authorised as vetting agencies for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearances.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(c)	Security clearances	Mandatory
148	Y	The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment before a citizenship eligibility waiver is considered for a non-Australian citizen who has a valid visa and work rights to work in an identified position.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	*Entities must, if the person is not an Australian citizen and has a valid visa with work rights, provide the authorised vetting agency with an eligibility waiver by:* *i. establishing an exceptional business requirement and conducting a risk assessment*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(di)	Security clearances	Mandatory
149	Y	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 maintains a record of all citizenship eligibility waivers approved.	PER	18. Security Clearances		31/10/2024	Retain-Split	*Entities must, if the person is not an Australian citizen and has a valid visa with work rights, provide the authorised vetting agency with an eligibility waiver by:* *i. establishing an exceptional business requirement and conducting a risk assessment, and* *ii. asking the accountable authority to consider and accept the risk of waiving the citizenship requirement (Note ii).* *Note ii: The accountable authority may delegate this decision to the Chief Security Officer.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(d)	Security clearances	Mandatory
150	Y	The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment (including seeking advice from the Authorised Vetting Agency), before a checkable background eligibility waiver is considered for a clearance subject assessed as having an uncheckable background.	PER	18. Security Clearances	All entities	31/10/2024	Retain-Split	Entities must, if the authorised vetting agency assesses that the person has an uncheckable background, provide the vetting agency with an eligibility waiver by: i. establishing an exceptional business requirement and conducting a risk assessment (including seeking the advice of the vetting agency), and ii. asking the accountable authority to consider and accept the risk of waiving the checkable background requirement *(Note iii)* . *Note iii: The accountable authority may delegate this decision to the Chief Security Officer.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 2(e)	Security clearances	Mandatory
151	Y	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 maintains a record of all checkable background eligibility waivers approved.	PER	18. Security Clearances	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
152	Y	The Authorised Vetting Agency provides the Sponsoring Entity with information to inform a risk assessment if a clearance subject has an uncheckable background and only issues a clearance if the Accountable Authority waives the checkable background requirement and provides the Authorised Vetting Agency with a copy of the waiver.	PER	18. Security Clearances	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must, if a clearance subject has an uncheckable background: i. provide the sponsoring entity with information to inform a risk assessment, and ii. only issue a clearance if the accountable authority waives the checkable background requirement (see Requirement 2e).	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(d)	Personnel security vetting standards	Mandatory
153	Y	The clearance subject's informed consent is given to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must seek informed consent from the clearance subject to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance.	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(b)	Personnel security vetting standards	Mandatory
154	Y	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by considering their integrity (i.e. the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Australian Government Personnel Security Adjudicative Standard.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must assess the clearance subject's eligibility and suitability to hold a security clearance by: i. for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearances, considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines (at Annex A)	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3 (c i)	Personnel security vetting standards	Mandatory
155	Y	The clearance subject's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance is assessed in accordance with the TOP SECRET-Privileged Access Standard.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must assess the clearance subject's eligibility and suitability to hold a security clearance by: ii. for TOP SECRET-Privileged Access security clearances, assessing their trustworthiness and commitment to Australia, its values and its democratic system of government (ie honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the TOP SECRET-Privileged Access Standard *(Note iv)*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3 (c ii)	Personnel security vetting standards	Mandatory
156	Y	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by conducting the minimum personnel security checks for the commensurate security clearance level.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must assess the clearance subject's eligibility and suitability to hold a security clearance by: iii. conducting minimum personnel security checks for a security clearance outlined below (see tab 'policy 12 table' tab)	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3 (c iii)	Personnel security vetting standards	Mandatory

157	Y	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by resolving any doubt in the national interest.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must assess the clearance subject's eligibility and suitability to hold a security clearance by: iv. resolving and doubt in the national interest	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3 (c iv)	Personnel security vetting standards	Mandatory
158	Y	Concerns that are identified during the vetting or security clearance suitability assessment process, that are not sufficient to deny a security clearance and where the related risks can be managed through conditions attached to the security clearance, the Authorised Vetting Agency must: • identify the clearance conditions • provide the sponsoring entity with information about the concerns to inform a risk assessment • only issue a conditional security clearance if the Accountable Authority and the clearance subject accept the clearance conditions. The Accountable Authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the Accountable Authority of the clearance conditions.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must, if security concerns are identified during the vetting or security clearance suitability assessment process that are not sufficient to deny a security clearance, and the related risks can be managed through conditions attached to the security clearance: i. identify the clearance conditions ii. provide the sponsoring entity with information about the security concerns to inform a risk assessment iii. only issue a conditional security clearance if the accountable authority and the clearance subject accept the clearance conditions *(Note vi)* . *Note vi: The accountable authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the accountable authority of the clearance conditions.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(e)	Personnel security vetting standards	Mandatory
159	Y	The Authorised Vetting Agency provides the sponsoring entity with any other relevant information of concern that is identified during the vetting process when advising them of the outcome of the security vetting process, to inform the sponsoring entity's risk assessment.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must, if any other relevant information of security concern is identified during the vetting process, provide the sponsoring entity with information to inform a risk assessment when advising them of the outcome of the security vetting process *(Note vii)* . *Note vii: Where security concerns are identified that may lead to an adverse recommendation, the vetting agency (while any determination is still pending, including where a clearance subject has been invited to respond to identified risks) shares only relevant information with the sponsoring entity to enable temporary mitigations until a final outcome is made. See Requirement 3e.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(f)	Personnel security vetting standards	Mandatory
160	Y	The Authorised Vetting Agency applies the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny a security clearance (including grant lower level) or grant a conditional security clearance, without compromising the national interest. *Note: Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security clearance suitability assessment.*	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain-Split	Authorised vetting agencies must, without compromising the national interest, apply the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny a security clearance (including grant lower level) or grant a conditional security clearance *(Note vii)* . *Note viii: Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security clearance suitability assessment.*	Personnel Security	12. Eligibility and suitability of personnel	Supporting requirement 3(g)	Personnel security vetting standards	Mandatory
161	Y	The Authorised Vetting Agency reviews the conditions of conditional security clearances annually.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must: iii. for conditional security clearances, review conditions annually	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(biii)	Security clearance maintenance	Mandatory
162	Y	The Authorised Vetting Agency reviews the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause).	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must: iv. review the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause), and	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(biv)	Security clearance maintenance	Mandatory
163	Y	The Authorised TOP SECRET-Privileged Access Vetting Agency implements the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must: v. implement the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(bv)	Security clearance maintenance	Mandatory
164	Y	The Sponsoring Entity actively assesses, monitors and manages the ongoing suitability of personnel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(a)	Security clearance maintenance	Mandatory
165	Y	The Sponsoring Entity monitors and manages compliance with any conditional security clearance requirements and reports any non-compliance to the Authorised Vetting Agency.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel, including by: iii. monitoring compliance with, and managing risk in relation to, clearance maintenance requirements for security clearance holders granted a conditional security clearance and reporting non-compliance to the authorised vetting agency	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(aiii)	Security clearance maintenance	Mandatory
166	Y	The Sponsoring Entity monitors and manages compliance with security clearance maintenance obligations for the clearance holders they sponsor.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	New (add)	In accordance with Requirement 1a, sponsoring entities must share information on any changes in circumstances of a clearance holder with the relevant authorised vetting agency. Table 3 provides guidance on entity responsibilities for assessing and managing changes in circumstances.	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(a) and paragraph 35	Collecting and assessing information on change of circumstances	Passive control
167	Y	The Sponsoring Entity shares relevant information of concern, where appropriate.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel, including by: i. collecting, assessing and sharing information of security concern	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(ai)	Security clearance maintenance	Mandatory
168	Y	The Sponsoring Entity conducts an annual security check with all security cleared personnel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel, including by: ii. conducting annual security checks with all security cleared personnel	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(aii)	Security clearance maintenance	Mandatory
169	Y	The Sponsoring Entity reviews eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel, including by: iv. reviewing eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(aiv)	Security clearance maintenance	Mandatory
170	Y	The Sponsoring Entity monitors, assesses and manages personnel with TOP SECRET-Privileged access security clearances in accordance with the TOP SECRET-Privileged Access Standard.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Sponsoring entities must actively monitor and manage the ongoing suitability of their security cleared personnel, including by: v. implementing the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged access security clearances.	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(av)	Security clearance maintenance	Mandatory
171	Y	The Authorised Vetting Agency reassess a clearance holder's eligibility and suitability to hold a security clearance by revalidating minimum personnel security checks for a security clearance.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must reassess a clearance holder's eligibility and suitability to hold a security clearance by: c. revalidating minimum personnel security checks for a security clearance outlined below (see 'policy 13 table' tab). Table: Minimum requirements for revalidation of security clearances	Personnel Security	13. Ongoing assessment of personnel	Supporting Requirement 2 (c)	Security clearance revalidation	Mandatory
172	Y	The Authorised Vetting Agency reassess a clearance holder's eligibility and suitability to hold a Baseline, Negative vetting 1, Negative Vetting 2 or Positive Vetting security clearance, by considering their integrity in accordance with the Australian Government Personnel Security Adjudicative Standard.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must reassess a clearance holder's eligibility and suitability to hold a security clearance by: a. for Baseline, Negative vetting 1, Negative Vetting 2 and Positive Vetting security clearances, considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines (see the PSPF policy: Eligibility and suitability of personnel Annex A)	Personnel Security	13. Ongoing assessment of personnel	Supporting Requirement 2 (a)	Security clearance revalidation	Mandatory

173	Y	The TOP SECRET-Privileged Access Vetting Authority reassess a clearance holder's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance, by, assessing their trustworthiness in accordance with the TOP SECRET-Privileged Access Standard.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must reassess a clearance holder's eligibility and suitability to hold a security clearance by: b. for TOP SECRET-Privileged Access security clearances, assessing their trustworthiness and commitment to Australia, its values and its democratic system of government (ie honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the TOP SECRET-Privileged Access Standard (Note ii). Note ii: The TOP SECRET-Privileged Access Standard contains specific guidance on the TOP SECRET-Privileged Access process. The TOP SECRET-Privileged Access Standard is available to TOP SECRET-Privileged Access practitioners and sponsoring entity Chief Security Officers via the TOP SECRET-Privileged Access Quality Assurance Office.	Personnel Security	13. Ongoing assessment of personnel	Supporting Requirement 2 (b)	Security clearance revalidation	Mandatory
174	Y	The Authorised Vetting Agency reassess a clearance holder's eligibility and suitability to hold a security clearance by resolving any doubt in the national interest.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must reassess a clearance holder's eligibility and suitability to hold a security clearance by: d. resolving any doubt in the national interest.	Personnel Security	13. Ongoing assessment of personnel	Supporting Requirement 2 (d)	Security clearance revalidation	Mandatory
175	Y	The Authorised Vetting Agency commences the security clearance revalidation process in sufficient time to complete the revalidation before the due date so that the security clearance does not lapse.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
176	Y	The Authorised Vetting Agency shares information of concern about security clearance holders with the Sponsoring Entity so they can decide whether to suspend or limit the clearance holder's access to Australian Government classified information, resources or activities until the concerns are resolved.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
177	Y	The Sponsoring Entity shares relevant information of security concern, where appropriate with the Authorised Vetting Agency.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain-Split	Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.	Personnel Security	13. Ongoing assessment of personnel	Core requirement	Ongoing suitability of personnel	Mandatory
178	Y	The Authorised Vetting Agency shares information of security concern about security clearance holders with the Sponsoring Entity.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must: i. share information of security concern about security clearance holders with sponsoring entities	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(bi)	Security clearance maintenance	Mandatory
179	Y	The Authorised Vetting Agency assesses and responds to information of security concern about security clearance holders, including reports from Sponsoring Entities.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain-Split	Vetting agencies must: ii. assess and respond to information of security concern about security clearance holders, which includes reports from sponsoring entities	Personnel Security	13. Ongoing assessment of personnel	Supporting requirement 1(bii)	Security clearance maintenance	Mandatory
180	Y	Negative Vetting 2 and higher clearance holders receive appropriate departmental travel briefings when undertaking international personal and work travel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A
181	Y	The Chief Security Officer, Chief Information Security Officer (or other relevant security practitioner) is advised prior to separation or transfer of any proposed cessation of employment resulting from misconduct or other adverse reasons.	PER	22. Separation	All entities	31/10/2024	Retain-Split	Prior to personnel separation or transfer, entities must: a. notify the Chief Security Officer, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons	Personnel Security	14. Separating personnel	Supporting requirement 1 a	Sharing security relevant information, debriefs and continuing obligations	Mandatory
182	Y	Separating personnel are informed of any ongoing security obligations under the *Commonwealth Criminal Code* and other relevant legislation and those holding a security clearance or access security classified information are debriefed prior to separation from the entity.	PER	22. Separation	All entities	31/10/2024	Retain	Each entity must ensure that separating personnel are informed of any ongoing security obligations.	Personnel Security	14. Separating personnel	Core requirement	Separating personnel obligations	Mandatory
183	Y	Separating personnel transferring to another Australian Government entity, the entity, when requested, provides the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks.	PER	22. Separation	All entities	31/10/2024	Retain-Split	Prior to personnel separation or transfer, entities must: c. for personnel transferring to another Australian Government entity, provide the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks	Personnel Security	14. Separating personnel	Supporting requirement 1c	Sharing security relevant information, debriefs and continuing obligations	Mandatory
184	Y	Separating personnel transferring to another Australian Government entity, the entity reports any security concerns (as defined in the in the *Australian Security Intelligence Organisation Act 197*9) to the Australian Security Intelligence Organisation.	PER	22. Separation	All entities	31/10/2024	Retain-Split	Prior to personnel separation or transfer, entities must: d. report any security (as defined in the in the Australian Security Intelligence Organisation Act 1979) concerns to the Australian Security Intelligence Organisation (ASIO). *Note: Requirements 1 and 2 apply to all personnel; this includes security cleared personnel, non-security cleared personnel, contractors and third party individuals*	Personnel Security	14. Separating personnel	Supporting requirement 1d	Sharing security relevant information, debriefs and continuing obligations	Mandatory
185	Y	A risk assessment is completed to identify any security implications in situations where it is not possible to undertake the required separation procedures.	PER	22. Separation	All entities	31/10/2024	Retain	Where it is not possible to undertake required separation procedures, entities must undertake a risk assessment to identify any security implications. *Note: Requirement 3 applies more broadly and in certain circumstances.*	Personnel Security	14. Separating personnel	Supporting requirement 3	Risk assessment	Mandatory
186	Y	Separating personnel have their access to Australian Government resources withdrawn upon separation or transfer from the entity, including information, technology systems, and resources.	PER	22. Separation	All entities	31/10/2024	Retain	Each entity must ensure that separating personnel have their access to Australian Government resources withdrawn.	Personnel Security	14. Separating personnel	Core requirement	Separating personnel obligations	Mandatory
187	Y	The Sponsoring Entity advises the relevant Authorised Vetting Agency of the separation of a clearance holder, including any relevant circumstances (e.g. termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, along with any identified risks or security concerns associated with the separation.	PER	22. Separation	All entities	31/10/2024	Retain-Split	Following the separation of security cleared personnel: a. sponsoring entities must advise the relevant authorised vetting agency of: i. the separation of a clearance holder, including any relevant circumstances (eg termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, and ii. any identified risks or security concerns associated with the separation, including as a result of Requirement 3. *Note: Requirement 4 applies to security cleared personnel*	Personnel Security	14. Separating personnel	Supporting requirement 4 (a)	Security clearance actions	Mandatory
188	Y	The Authorised Vetting Agency manages and records changes in the security clearance status of separating personnel, including a change of Sponsoring Entity, and transfer personal security files where a clearance subject transfers to an entity covered by a different Authorised Vetting Agency, to the extent that their enabling legislation allows.	PER	22. Separation	Authorised Vetting Agency	31/10/2024	Retain-Split	Following the separation of security cleared personnel: b. authorised vetting agencies must: i. manage and record changes in the security clearance status of separating personnel, including a change of sponsoring entity, and ii. transfer personal security files where a clearance subject transfers to an entity covered by a different authorised vetting agency, to the extent that their enabling legislation allows. *Note: Requirement 4 applies to security cleared personnel*	Personnel Security	14. Separating personnel	Supporting requirement 4 (b)	Security clearance actions	Mandatory
189	Y	Protective security is integrated in the process of planning, selecting, designing and modifying entity facilities for the protection of people, information and resources.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Each entity must ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets.	Physical Security	16. Entity facilities	Core requirement (a)	Protective security in facility planning	Mandatory
190	Y	A facility security plan is developed for new facilities, facilities under construction or major refurbishments of existing facilities.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	New (add)	The Department of Home Affairs recommends that entities develop a site security plan for new facilities, including facilities under construction or major refurbishments of existing facilities	Physical Security	16. Entity facilities	Paragraph 4	Site Planning	Recommended
191	Y	Decisions on entity facility locations are informed by considering the site selection factors for Australian Government facilities.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	New (add)	N/A new requirement	N/A	N/A	N/A	N/A	N/A

192	Y	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.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	When designing or modifying facilities, entities must secure and control access to facilities to meet the highest risk level to entity resources. When designing or modifying facilities, entities must define restricted access areas as detailed below. Zone name -- Zone definition Zone One -- Public access. Zone Two -- Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control. Zone Three -- No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control. Zone Four -- No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control. Zone Five -- No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control	Physical Security	16. Entity facilities	Requirement 1 (a & b)	Design and modify facilities	Mandatory
193	Y	Facilities are constructed in accordance 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.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Entities must ensure security zones are constructed to protect against the highest risk level in accordance with the entity security risk assessment in areas: i. accessed by the public and authorised personnel, and ii. where physical assets, other than security classified assets, are stored.	Physical Security	16. Entity facilities	Supporting requirement 2(b)	Building construction	Mandatory
194	Y	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.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Entities must ensure facilities for Zones Two to Five that store security classified information and assets are constructed in accordance with applicable sections of: i. ASIO Technical Note 1/15 – Physical Security Zones, and ii. ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas	Physical Security	16. Entity facilities	Supporting requirement 2(a)	Building construction	Mandatory
195	Y	Entity facilities are operated and maintained in accordance with Security Zones and Physical Security Measures and Controls.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Modify	Coverage for content in existing Supporting requirements 3, 4, 5, and 6.	Physical Security	16. Entity facilities	Supporting requirements (3, 4, 5, and 6)	Individual control elements	Mandatory
196	Y	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.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	CSOs or delegated security advisers must, before using a facility operationally, certify the facility's Zones One to Four in accordance with the PSPF and ASIO Technical Notes	Physical Security	16. Entity facilities	Supporting requirement 7 (a)	Security zone certification	Mandatory
197	Y	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.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	CSOs or delegated security advisers must, before using a facility operationally, for Zone Five facilities, obtain: i. ASIO-T4 physical security certification for security areas used to handle TOP SECRET security classified information, sensitive compartmented information (SCI) or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level.	Physical Security	16. Entity facilities	Supporting requirement 7 (b)	Security zone certification	Mandatory
198	Y	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.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	CSOs or delegated security advisers must, before using a facility operationally, accredit Zones One to Five when the security controls are certified and the entity determines and accepts the residual risks.	Physical Security	16. Entity facilities	Supporting requirement 8 (a)	Security zone accreditation	Mandatory
199	Y	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.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	CSOs or delegated security advisers must, before using a facility operationally, for Zone Five facilities, obtain: i. Australian Signals Directorate security accreditation for areas used to secure and access TOP SECRET sensitive compartmented information.	Physical Security	16. Entity facilities	Supporting requirement 8 (b)	Security zone accreditation	Mandatory
200	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	Each entity must implement physical security measures that 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.	Physical Security	15. Physical security for entity resources	Core requirement (b)	Physical security measures	Mandatory
201	Y	Physical security measures are implemented to protect entity resources, commensurate with the assessed business impact level of their compromise, loss or damage.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	retain	Entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, *(Note i)* loss or damage. *Note i: Information compromise is defined in PSPF policy: Classification system.*	Physical Security	15. Physical security for entity resources	Supporting requirement 1	Physical security measures	Mandatory
202	Y	Physical security measures are implemented to minimise or remove the risk of harm to people.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	Each entity must implement physical security measures that minimise or remove the risk of harm to people.	Physical Security	15. Physical security for entity resources	Core requirement (a)	Physical security measures	Mandatory
203	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Modify	Entities must assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.	Physical Security	15. Physical security for entity resources	Supporting requirement 2	Security containers, cabinets and rooms	Mandatory
204	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Entities must, in areas that store security classified information, ensure perimeter doors and hardware are: a. constructed in accordance with ASIO Technical Notes in Zones Two to Five, and b. secured with SCEC-approved products rated to Security Level 3 in Zones Three to Five	Physical Security	16. Entity facilities	Requirement 3 (a & b)	Hardware	Mandatory
205	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	Entities must control access to Zones Two to Five within the entity's facilities by only allowing access for authorised personnel, visitors, vehicles and equipment and apply the following controls: i. for Zones Two to Five, use: A. electronic access control systems where there are no other suitable identity verification and access control measures in place. ii. for Zones Three to Five, use: A. identity cards with personal identity verification B. sectionalised access control system with full audit C. regular review of audit logs for any unusual or prohibited activity iii. for Zone Four and Zone Five, ensure access control systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. privileged operators and users are appropriately trained and security cleared to the level of the security zone, and iv. for Zone Five, use dual authentication access control.	Physical Security	16. Entity facilities	Supporting requirement 5 (a)	Access control	Mandatory

206	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	Entities must control access to Zones Two to Five within the entity's facilities by only allowing access for authorised personnel, visitors, vehicles and equipment and apply the following controls: i. for Zones Two to Five, use: A. electronic access control systems where there are no other suitable identity verification and access control measures in place. ii. for Zones Three to Five, use: A. identity cards with personal identity verification B. sectionalised access control system with full audit C. regular review of audit logs for any unusual or prohibited activity iii. for Zone Four and Zone Five, ensure access control systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. privileged operators and users are appropriately trained and security cleared to the level of the security zone, and iv. for Zone Five, use dual authentication access control.	Physical Security	16. Entity facilities	Supporting requirement 5 (a)	Access control	Mandatory
207	Y	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.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	When granting ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, the entity's accountable authority or CSO must ensure the person has: i. the required level of security clearance for the facility's security zones, and ii. a business need supported by a business case and risk assessment, which is reassessed on a regular basis at least every two years.	Physical Security	16. Entity facilities	Supporting requirement 5 (b)	Access control	Mandatory
208	Y	Unauthorised access to Security Zones One to Five is controlled in accordance with the physical security measures and controls for security alarm systems.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	(a) Entities must for Zone Three, use either: i. a Type 1A security alarm system, or ii. a Class 5 commercial security alarm system, or iii. guard patrols performed at random intervals and within every four hours. (b) Entities must, for Zone Four and Zone Five, use: i. SCEC-approved Type 1A security alarm system in accordance with the Type 1A security alarm system transition policy with SCEC-approved detection devices, and ii. a SCEC-endorsed Security Zone Consultant to design and commission the SCEC approved Type 1A alarm system. (c) Entities must, in Zones Three (Note i) to Five: i. use sectionalised security alarm systems ii. security alarm systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. monitored and responded to in a timely manner, and iii. privileged alarm systems operators and users are appropriately trained and security cleared. Note i: Unless guard patrols are used instead of a security alarm system in accordance with Requirement 4aiii.	Physical Security	16. Entity facilities	Supporting requirement 4	Security alarm systems	Mandatory
209	Y	Security guard arrangements in Security Zones One to Five are established in accordance with the physical security measures and controls for security guards.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain-Split	security guard elements from Requirement 4	Physical Security	16. Entity facilities	Supporting requirement 4	Security alarm systems	Mandatory
210	Y	Technical surveillance countermeasures for Security Zones One to Five are established in accordance with the physical security measures and controls for technical surveillance countermeasures.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Entities must ensure a technical surveillance countermeasures inspection is completed for facilities where: a. TOP SECRET discussions are regularly held, or b. the compromise of discussions may have a catastrophic business impact level.	Physical Security	16. Entity facilities	Supporting requirement 6	Technical surveillance counter-measures	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	International agreements and arrangements commonly require that security assessment visits have prior written approval from the Department of Home Affairs or a Competent Security Authority. Visits will only be approved for foreign government personnel who have a valid level of Australian or foreign government security clearance for access to the foreign government information and assets in the facility.	Security Governance	07. Security governance for international sharing	Paragraph 36	Foreign visits	Passive control
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The originator must remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity must not remove or change information's classification without the originator's approval.					
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Entities must ensure that contracts for goods and services include relevant security terms and conditions for the provider to manage identified security risks relevant to the procurement.	Security Governance	06. Security governance for contracted goods and service providers	Supporting Requirement 2	Establishing protective security terms and conditions in contracts	Mandatory
N/A	N	Critical people and resources - The security plan must identify people and resources that are critical to the ongoing operation of the entity and the national interest and detail the protections applied to protect these resources to support the continuity of the entity's core business. Resources covers information, systems, assets and facilities.	GOV	03. Security Planning, Incidents and Training	All entities		Retain	Entities must identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources to support their core business.	Security Governance	03. Security planning and risk management	Supporting requirement 2	Critical assets	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	On separation or transfer, entities must remove personnel's access to Australian Government resources, including: a. physical facilities, and b. ICT systems. *Note: Requirements 1 and 2 apply to all personnel; this includes security cleared personnel, non-security cleared personnel, contractors and third party individuals.*	Personnel Security	14. Separating personnel	Supporting requirement 2	Withdrawal of access	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must report on security each financial year to its portfolio minister and the Department of Home Affairs addressing key security risks to the entity's people, information and assets.	Security Governance	05. Reporting on security	Core requirement (aiii)	Reporting	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Entities must document and evidence their assessment of the entity's security maturity.	Security Governance	04. Security maturity monitoring	Supporting requirement 1	Security maturity records	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Entities must ensure information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in Annexes A-C.	Information Security	08. Classification System	Supporting Requirement 7 (b)	Minimum protections and handling requirements	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must: i. **identify information holdings**	Information Security	08. Classification System	Core requirement (i)	Information holdings	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Entities must not expose the public to unnecessary security risks when they transact online with government.	Information Security	10. Safeguarding data from cyber threats	Supporting Requirement 1	Transacting online with the public	Mandatory

N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must in areas where security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes.	Physical Security	16. Entity facilities	Core requirement (b)	Certification of physical security zones	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must accredit its security zones.	Physical Security	16. Entity facilities	Core requirement (c)	Accredication of physical security zones	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The originator must clearly identify security classified information, including emails, using applicable protective markings by, if text-based protective markings cannot be used, using colour-based protective markings.	Information Security	08. Classification System	Supporting Requirement 4 (b)	Marking information	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The originator must clearly identify security classified information, including emails, using applicable protective markings by, if text or colour-based protective markings cannot be used (eg verbal information), applying the entity's marking scheme for such scenarios. Entities must document a marking scheme for this purpose and train personnel appropriately.	Information Security	08. Classification System	Supporting Requirement 4 (c)	Marking information	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must report on security each financial year to its portfolio minister and the Department of Home Affairs addressing the maturity of the entity's security capability.	Security Governance	05. Reporting on security	Core requirement (aii)	Reporting	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must report on security each financial year to its portfolio minister and the Department of Home Affairs addressing details of measures taken to mitigate or otherwise manage identified security risks.	Security Governance	05. Reporting on security	Core requirement (aiv)	Reporting	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must complete the Australian Signals Directorate's annual cyber security survey.	Security Governance	05. Reporting on security	Core requirement (c) and Supporting requirement 3	ASD cyber security survey	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The accountable authority of each entity must manage the security risks of their entity	Security Governance	01. Role of accountable authority	Core requirement	Protective security leadership	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The accountable authority must empower the CSO to make decisions about: i. appointing security advisors within the entity ii. the entity's protective security planning iii. the entity's protective security practices and procedures iv. investigating, responding to, and reporting on security incidents	Security Governance	02. Management structures and responsibilities	Core requirement (b)	Security leadership	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	The accountable authority must empower the CISO to make decisions about: i. the entity's cyber security strategy and associated implementation program ii. appointing cyber security advisors within the entity iii. the entity's data and systems that process, store or communicate data iv. the entity's implementation of the Information Security Manual v. investigating, responding to, and reporting on cyber incidents	Security Governance				
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	a. The CSO must be responsible for directing all areas of security to protect the entity's people, information and assets. This includes appointing security advisors to support them in the day to-day delivery of protective security and, to perform specialist services.	Security Governance	02. Management structures and responsibilities	Supporting requirement 1 (a)	Security advisors	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	b. The CISO must be responsible for the entity's cyber security program and associated implementation program. This includes appointing cyber security advisors to support them in the day-to-day delivery of cyber security, and to perform specialist services.	Security Governance	02. Management structures and responsibilities	Supporting requirement 1 (b)	Security advisors	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	When conducting a security risk assessment, entities must communicate to the affected Commonwealth entity any identified risks that could potentially impact on the business of another entity	Security Governance	03. Security planning and risk management	Supporting requirement 4	Impact of risks	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must report on security to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation	Security Governance	05. Reporting on security	Core requirement (b)	Reporting	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must: **ii. assess the security classification of information holdings, and**	Information Security	08. Classification System	Core requirement (ii)	Information holdings	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	Each entity must submit a report on security each financial year: a. through the PSPF online reporting portal for information up to PROTECTED **or** b. by submitting an offline reporting template for information classified higher than PROTECTED.	Security Governance	05. Reporting on security	Supporting requirement 1	PSPF reporting model and template	Mandatory
N/A	N	N/A	N/A	N/A	N/A	N/A	Remove	empower the CISO to make decisions about: i. the entity's cyber security strategy and associated implementation program ii. appointing cyber security advisors within the entity iii. the entity's data and systems that process, store or communicate data iv. the entity's implementation of the Information Security Manual v. investigating, responding to, and reporting on cyber incidents. 32. Under the core requirement and Requirement 1(a), the CSO is empowered to appoint security advisors and Requirement 1(b), the CISO is empowered to appoint cyber security advisors. In making these decisions, the CSO and CISO are encouraged to: determine the appropriate competencies, experience and specialist skills or qualifications required to undertake the appointed security role/s, including comprehensive knowledge of the PSPF	Security Governance	02. Management structures and responsibilities	Core requirement (d)	Appointing cyber security advisors	Mandatory
Table 1	Y	Security goals and objectives - The security plan must detail the entity's security goals and strategic objectives, including how security risk management intersects with and supports broader business objectives and priorities.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities.	Security Governance	03. Security planning and risk management	Core requirement (a)	Security plan	Mandatory
Table 1	Y	Security risk environment -The security plan must detail the environment in which the entity operates; the threats, risks and vulnerabilities that impact the protection of the entity's people, information and resources, including: The Accountable Authority has overall responsibility for managing: • what the entity needs to protect (via a risk assessment) being the people, information and resources assessed as critical to its ongoing operation and to the national interest • what it needs to protect against (via threat assessment) • how security risks will be managed within the entity.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets	Security Governance	03. Security planning and risk management	Core requirement (b)	Security plan	Mandatory
Table 1	Y	Risk tolerance - The security plan must detail the entity's tolerance to security risks, agreed by the Accountable Authority (see 5.1). Each entity's level of tolerance for risk will vary depending on the level of potential damage to the Australian Government or to the entity.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the entity's tolerance to security risks	Security Governance	03. Security planning and risk management	Core requirement (c)	Security plan	Mandatory
Table 1	Y	Security capability - The security plan must detail the maturity of the entity's capability to manage security risks.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the maturity of the entity's capability to manage security risks	Security Governance	03. Security planning and risk management	Core requirement (d)	Security plan	Mandatory

Table 1	Y	Security risk management strategies - The security plan must detail the entity's mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances, and strategies to implement security risk management and maintain a positive risk culture. The entity's approach to managing security risks, including identifying how it will apply proportional and sufficient controls to deter, detect, delay and respond to threats (internal or external) that affect the security of its people, information or assets. This includes: • establishing risk stewards and managers • instigating steps that minimise risks (according to risk environment and tolerances) • managing residual risks to ensure the protection of people, information and resources.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the entity's strategies to implement security risk management and maintain a positive risk culture	Security Governance	03. Security planning and risk management	Core requirement (e)	Security plan	Mandatory
Table 1	Y	PSPF implementation - The security plan must detail the entity's strategies to deliver against the PSPF requirements and standards.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail entity's strategies to deliver against the PSPF	Security Governance	03. Security planning and risk management	Core requirement (e)	Security plan	Mandatory
Table 1	Y	PSPF Directions - The security plan must detail the entity's arrangements for implementing any direction issued by the Secretary of the Department of Home Affairs under the PSPF. This includes the entity's approach to implementing the requirements specified in any directions, as well as to ensure any timeframes or additional reporting obligations specified in the direction are met. If the direction allows, this may include the entity's arrangements to implement alternative mitigations.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan must detail the entity's arrangements for implementing any direction issued by the Secretary of the Department of Home Affairs under the PSPF.	Security Governance	03. Security planning and risk management	Core requirement (f)	Security plan	Mandatory
Table 1	Y	Threat levels - The security plan must be calibrated to the security environment in which the entity operates, including the National Terrorism Threat Level and relevant ASIO reporting related to espionage, foreign interference or sabotage threats. The plan should promote flexibility and scalable security controls which can be calibrated to changes in the security environment.	GOV	03. Security Planning, Incidents and Training	All entities	N/A	Retain	The security plan (and supporting security plans) must include scalable measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.	Security Governance	03. Security planning and risk management	Supporting requirement 5	Threat levels	Mandatory