



DISP Membership Requirements Checklist

2026 Edition

A structured self-assessment guide for Australian entities applying for DISP membership. Content aligned to the official Defence Industry Security Program requirements as published by the Defence Industry Security Office (DISO).

4 Security Domains · 22 Requirements · E8 ML2 Mandate (Nov 2025) · All Membership Levels

dispmembership.com.au · seriousdefence.com.au · April 2026

HOW TO USE THIS CHECKLIST

This checklist is based on the official **DISP Membership Requirements Checklist** published by the Department of Defence (defence.gov.au). It is designed to help you assess how closely your business currently meets DISP membership requirements and to identify any gaps you will need to address before submitting your application through the **Defence Supplier Portal (DSP)**.

TAG	MEANING
ALL	Required at all membership levels, including Entry Level
L1+	Required at Level 1 and above (PROTECTED classification)
L2+	Required at Level 2 and above (SECRET classification)
L3	Level 3 only (TOP SECRET classification)

Important: This checklist covers the four official DISP security domains. DISP membership levels align with Australian Government security classifications: Entry Level (OFFICIAL/OFFICIAL:Sensitive), Level 1 (PROTECTED), Level 2 (SECRET), and Level 3 (TOP SECRET). Always verify current requirements with DISO at disp.info@defence.gov.au or call **1800 Defence (1800 333 362)**.

How Serious Defence can help: Serious Defence offers three purpose-built products to accelerate your DISP journey. **DISPulse** is Australia's first DISP GRC platform — it automates your Annual Security Report, tracks control status across all four domains, and generates evidence packages for DISO review. **DISPeer** provides a sovereign, Australian-hosted ICT environment pre-configured to meet DISP ICT security requirements, eliminating the Essential Eight ML2 build burden. **DISPath** is our guided compliance consulting service — ideal for organisations working through this checklist for the first time. Learn more at dispmembership.com.au.

01

GOVERNANCE

9 requirements

REQUIREMENT / QUESTION	RESPONSE	GUIDANCE / COMMENT	LEVEL
Does your organisation have a nominated Chief Security Officer (CSO) who is accountable for the security of your business?	Yes / No	A CSO must be in place prior to submitting your application. The CSO is accountable to the governing body for all security matters.	ALL
Does your organisation have a nominated Security Officer (SO) ? (The SO can be the same person as the CSO.)	Yes / No	A SO must be in place prior to submitting your application. The SO manages day-to-day security operations and DISP reporting obligations.	ALL
Does your CSO/SO hold a security clearance, and if so, at what level?	Specify clearance level or N/A	If no clearance is held, you can still submit your application — DISO will assist with the clearance process for your CSO/SO.	ALL
Does your business have security policies and plans in place at the appropriate DISP membership level, which will be maintained and made available to Defence on request?	Yes / No	Security policies and plans must be documented prior to submitting your application. Templates are available from the Security Officer Toolkit on the DISP Resources page (defence.gov.au).	ALL
Does your business run an annual security awareness programme for all staff at the appropriate DISP membership level, available to Defence on request?	Yes / No	If not yet in place, you can still apply — DISO will assist. DISPulse includes a built-in training register and awareness programme module.	ALL
Does your business have an insider threat awareness programme for all staff at the appropriate DISP membership level, available to Defence on request?	Yes / No	If not yet in place, you can still apply — DISO will assist. An insider threat policy template is included in the DISP Security Policies and Plans templates.	ALL

REQUIREMENT / QUESTION	RESPONSE	GUIDANCE / COMMENT	LEVEL
Do the CSO and SO commit to their DISP reporting obligations and will they maintain a register of security incident reports, contact reports, and overseas travel briefings, available to Defence on request?	Yes / No	If not yet in place, DISO will assist including providing document templates. DISPulse automates incident reporting, foreign contact registers, and travel briefing workflows.	ALL
Does your entity have a mechanism for the governing body, through the CSO, to approve and submit the Annual Security Report (ASR) annually?	Yes / No	An ASR mechanism must be established and documented prior to submitting your application. An ASR template is available from the DISP Resources page. DISPulse generates your ASR with one click.	ALL
If applying for Level 1 or above, does your business maintain a list of Designated Security Assessed Positions (DSAP) available to Defence on request? (A DSAP is a position or role requiring access to classified material.)	Yes / No	For Level 1 and above, a DSAP register must be in place prior to submitting your application. A security register template incorporating a DSAP section is available from the Security Officer Toolkit.	L1+

DISPulse

DISP GRC Platform — dispmembership.com.au/dispulse

DISPulse automates your Annual Security Report, tracks governance control status in real time, manages your incident register, foreign contact register, and overseas travel briefings — and generates evidence packages ready for DISO review. Purpose-built for Australian DISP members.

02

PERSONNEL SECURITY

6 requirements

REQUIREMENT / QUESTION	RESPONSE	GUIDANCE / COMMENT	LEVEL
Will all future business employment practices meet or exceed the requirements of employment screening standard AS 4811:2022 , and be made available to Defence upon request?	Yes / No	This must be in place and documented prior to submitting your application. AS 4811:2022 covers pre-employment screening including identity, right to work, criminal history, and reference checks.	ALL
Does the SO agree to support security clearance holders to uphold their clearance responsibilities? This includes submitting change of circumstance forms, security reports, and conducting overseas travel briefings.	Yes / No	You will need to establish and document a process to support this prior to submitting your application.	ALL
Will your people be working in a Defence establishment ?	Yes / No	If yes, they will need a security clearance at the level specified by Defence for that establishment.	ALL
Do your employees need a security clearance ?	Yes / No	Entry Level: clearances are sponsored by Defence or another government agency. Level 1: BASELINE (PROTECTED). Level 2: NV1 (SECRET). Level 3: NV2 (TOP SECRET).	ALL
Does your business require the ability to sponsor and manage security clearances ?	Yes / No	Entry Level membership does not include the ability to sponsor clearances — these are sponsored by Defence. Sponsorship capability is available from Level 1 upward.	L1+
If yes, what level of security clearance does your business need to sponsor?	Specify level(s)	Level 1: BASELINE (PROTECTED). Level 2: NV1 (SECRET). Level 3: NV2 (TOP SECRET). Confirm the highest clearance level required for your contracts.	L1+

DISPath

Guided Compliance Consulting — dispmembership.com.au/dispath

DISPath's personnel security module helps you establish AS 4811:2022-compliant screening procedures, build your DSAP register, and prepare clearance sponsorship workflows. Our consultants have supported 50+ DISP engagements across Australian and UK defence supply chains.

03

PHYSICAL SECURITY

4 requirements

REQUIREMENT / QUESTION	RESPONSE	GUIDANCE / COMMENT	LEVEL
Does your business need to use classified information and/or assets ?	Yes / No	Entry Level: OFFICIAL/OFFICIAL:Sensitive. Level 1: PROTECTED. Level 2: SECRET. Level 3: TOP SECRET. The classification level determines your physical security obligations.	ALL
What is the highest level of classification your business needs to use?	Specify classification	Entry Level: OFFICIAL/OFFICIAL:Sensitive. Level 1: PROTECTED. Level 2: SECRET. Level 3: TOP SECRET. Physical security controls must match the highest classification handled.	ALL
Does your business have a clear access control policy and permissions in practice?	Yes / No	Access control policies must be in place and documented prior to submitting your application. This includes physical access to areas where classified material is handled or stored.	ALL
Does your access control extend to any third-party providers of goods and services ?	Yes / No	If yes, third parties must also meet the membership requirements for the appropriate DISP level, OR be appropriately risk-managed by the prime contractor via a security risk assessment.	ALL

DISPath

Physical Security Assessment — dispmembership.com.au/dispath

DISPath includes physical security assessment templates and facility security planning workflows aligned to DSPF zone classification requirements (public, restricted, controlled). Our team can conduct on-site assessments and prepare the physical security documentation required for your DISO submission.

04

INFORMATION & CYBER SECURITY

3 requirements

REQUIREMENT / QUESTION	RESPONSE	GUIDANCE / COMMENT	LEVEL
Will your information networks need to handle classified information ?	Yes / No	Entry Level: OFFICIAL/OFFICIAL:Sensitive. Level 1: PROTECTED. Level 2: SECRET. Level 3: TOP SECRET. ICT security controls must match the highest classification stored, processed, or communicated.	ALL
What is the highest level of classified information your business needs to store, process, or communicate?	Specify classification	Entry Level: OFFICIAL/OFFICIAL:Sensitive. Level 1: PROTECTED. Level 2: SECRET. Level 3: TOP SECRET. This determines your ICT accreditation obligations.	ALL
What cyber security standard does your corporate network meet? To be eligible for DISP membership, your ICT network must meet one of the listed accreditation standards.	Select applicable standard(s)	Accepted standards: ASD Essential Eight ML2 (Australian — mandatory from Nov 2025); NIST SP 800-171 (US); Def Stan 05-138 (UK); ISO/IEC 27001 and 27002 (International). See eligibility page at defence.gov.au .	ALL

Essential Eight ML2 — Mandatory from 15 November 2025

As of 15 November 2025, all DISP applicants and existing members are required to operate at **ASD Essential Eight Maturity Level 2 (ML2)** across all eight mitigation strategies. This applies at all membership levels including Entry Level. An ML2 assessment report (conducted within the past 12 months) must be included in your DISP application.

The Eight Strategies:

1. Application Control
2. Patch Applications
3. Configure Microsoft Office Macro Settings
4. User Application Hardening
5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-Factor Authentication
8. Regular Backups

DISPeer

Sovereign ICT Environment — dispmembership.com.au/dispeer

DISPeer is a fully managed, Australian-hosted cloud environment pre-configured to meet DISP ICT security requirements. It eliminates the Essential Eight ML2 build burden by providing a PROTECTED-ready workspace — your team connects securely without needing to build and maintain your own compliant ICT infrastructure.

NEXT STEPS		
01	Complete this checklist	Work through each domain and mark your current status. Identify gaps that need to be addressed before you apply.
02	Download official templates	Security Policies and Plans templates, the Security Register, and the ASR template are available free from the DISP Resources page at defence.gov.au .
03	Commission an E8 ML2 assessment	Engage a qualified assessor (IRAP-assessed assessor preferred for Level 2+) to conduct your Essential Eight ML2 assessment. The report must be current (within 12 months) at time of application.
04	Submit via the Defence Supplier Portal	Applications are submitted through the Defence Supplier Portal (DSP). The 'How to Complete a DISP Membership Application' guide is available from the DISP Resources page.
05	Prepare for the DISO assessment interview	Your Security Officer should be briefed and prepared to discuss your security posture with DISO. DISPath can conduct a pre-submission review and mock interview preparation.

Serious Defence dispmembership.com.au seriousdefence.com.au	Defence Industry Security Office (DISO) disp.info@defence.gov.au 1800 Defence (1800 333 362)	Official DISP Resources defence.gov.au/business-industry/industry-governance/.../disp/resources
--	---	---

This checklist is provided for guidance purposes only and does not constitute legal or security advice. DISP requirements are subject to change — always verify current requirements with the Defence Industry Security Office (DISO) and the Defence Security Principles Framework (DSPF). Content sourced from the official DISP Membership Requirements Checklist (defence.gov.au, November 2023) and updated to reflect the November 2025 Essential Eight ML2 mandate. Serious Defence Pty Ltd accepts no liability for decisions made on the basis of this document. Version 2.0 — April 2026.