Information Security Policy

Tarralea Digital Pty Ltd

Document ID	SEC-POL-01
Version	4.0
Classification	PROTECTED
Document owner	Chief Information Security Officer
Approved by	Board of Directors
Effective date	1 April 2026
Next review	1 April 2027
Applies to	Tarralea Digital Pty Ltd and all systems operated by it, including TARRALEA-PROTECTED and Tarralea corporate systems

1. Purpose

This policy establishes the governance arrangements, accountabilities and decision rights for cyber security at Tarralea Digital Pty Ltd ("Tarralea"). It applies to TARRALEA-PROTECTED, the PROTECTED-classified hosting environment operated by Tarralea for Australian Government agency workloads, and to Tarralea's corporate systems (classified OFFICIAL: Sensitive).

Tarralea is a member of the Defence Industry Security Program (DISP) at Level 1 across the governance, personnel, physical, and information and cyber security domains, and provides services to the Department of Defence. Tarralea is therefore bound by both the Australian Government Information Security Manual (ISM) and the Defence Security Principles Framework (DSPF). This policy is consistent with the ISM cyber security principles, gives effect to Tarralea's obligations as a DISP member under DSPF Control 16.1, and is supported by the standards, plans and procedures listed in Section 7.

2. Scope

This policy covers the establishment of cyber security authority, accountability and reporting within Tarralea. The technical and operational requirements for individual control domains are set out in the supporting documents at Section 7.

3. Governance and accountability

3.1 The Board of Directors is accountable for cyber security at Tarralea (GOV-01).

3.2 The Board of Directors discharges its cyber security oversight through the Audit, Risk and Compliance Committee (ARCC), a standing subcommittee of the Board.

3.3 The Chief Executive Officer is responsible for the implementation of this policy across Tarralea.

3.4 The Chief Information Security Officer (CISO) provides leadership and oversight of cyber security activities at Tarralea and owns this policy (GOV-02; ISM-0714; ISM-1478).

3.5 The Chief Information Security Officer chairs the Cyber Security Steering Committee (CSSC), which comprises the Chief Executive Officer, the Chief Operating Officer, the Head of Security Operations, the Platform Owner and the Chief Information Security Officer, and which meets formally each month (ISM-0725).

3.6 The Chief Information Security Officer develops, implements, maintains and regularly verifies the register of systems operated by Tarralea (ISM-1966). The Cyber Security Steering Committee uses the register of systems when approving the authorisation to operate for each system (see 5.2).

3.7 As a DISP member, Tarralea appoints a Chief Security Officer (CSO) and a Security Officer (SO) in accordance with DSPF Control 16.1. The Chief Information Security Officer also fulfils the role of Chief Security Officer for Tarralea's DISP membership; the two roles are held by the same person and carry a single set of responsibilities.

3.8 The Security Officer is appointed under the Chief Security Officer, undertakes the day-to-day management of protective security, and reports to the Chief Security Officer (DSPF Control 16.1).

3.9 The Chief Security Officer is the authority for Tarralea's security posture, including the acceptance of security risk affecting Tarralea's ability to protect Defence information and assets held on TARRALEA-PROTECTED (DSPF Control 16.1, paragraphs 63 and 66).

4. Reporting

4.1 The Chief Information Security Officer reports directly to the Board of Directors on cyber security matters at each Board meeting (ISM-0718).

4.2 The Chief Information Security Officer reports directly to the Audit, Risk and Compliance Committee on cyber security matters (ISM-1918).

4.3 The Chief Information Security Officer produces a quarterly cyber security report covering Tarralea's security risk profile, the status of key systems, outstanding security risks and recent cyber security incidents. The Audit, Risk and Compliance Committee reviews the quarterly cyber security report at each meeting and directs remediation priorities arising from it.

5. System authorisation and risk acceptance

5.1 Each system operated by Tarralea has a designated system owner (ISM-1071). The Platform Owner is the system owner for TARRALEA-PROTECTED.

5.2 The Authorising Officer for the TARRALEA-PROTECTED platform is the Chief Operating Officer. Following each security assessment, the Authorising Officer accepts the residual security risk for the TARRALEA-PROTECTED platform and grants its authorisation to operate (GOV-05; ISM-0027).

5.3 Residual security risk for Tarralea corporate systems is accepted by the Chief Executive Officer prior to their authorisation to operate.

5.4 The Platform Owner obtains an authorisation to operate for the TARRALEA-PROTECTED platform before it is brought into service and whenever a significant change is made to it (ISM-0027).

5.5 The certification and accreditation of TARRALEA-PROTECTED for the information and cyber security domain, required to receive, store and process PROTECTED information, is provided by the Defence Cyber and Information Assurance Branch (DCIAB) under DSPF Principle 23 — Cyber Security Assessment and Authorisation. Tarralea relies on this accreditation as the authorisation for TARRALEA-PROTECTED to handle PROTECTED information.

5.6 The Authorising Officer's authorisation under clause 5.2 covers the physical and infrastructure controls of the TARRALEA-PROTECTED platform.

6. Mandatory control requirements

6.1 **System hardening.** All systems operated by Tarralea are configured and hardened in accordance with the System Hardening and Configuration Management Standard (SEC-STD-04).

6.2 **Access recertification.** Access to all PROTECTED systems is reviewed and recertified at least every six months, in accordance with the Access Control and Identity Management Standard (SEC-STD-02).

6.3 **External incident reporting.** All cyber security incidents assessed as Critical are reported to the Defence security incident centre, in accordance with DSPF Control 77.1 — Security Incidents and Investigations, and to the Australian Signals Directorate under the ISM. Both reports are made in

accordance with the Cyber Security Incident Response Plan (SEC-PLN-03).

6.4 **Incident management.** Cyber security incidents are managed and a cyber security incident register is maintained in accordance with the Cyber Security Incident Response Plan (SEC-PLN-03) (ISM-0125).

7. Supporting documents

ID	Title
SEC-STD-02	Access Control and Identity Management Standard
SEC-PLN-03	Cyber Security Incident Response Plan
SEC-STD-04	System Hardening and Configuration Management Standard
SEC-PRO-05	Security Assurance and Monitoring Procedure

8. Review

The Chief Information Security Officer reviews this policy at least annually and following any significant change to Tarralea's operating environment or threat profile.

Version history

Version	Date	Author	Summary
1.0	Mar 2024	CISO	Initial issue
2.0	Apr 2025	CISO	Aligned to revised ISM cyber security principles
3.0	Jan 2026	CISO	Added TARRALEA-PROTECTED authorisation arrangements
3.1	Apr 2026	CISO	Annual review; minor corrections
4.0	Jun 2026	CISO	Incorporated DISP and DSPF obligations following DISP Level 1 membership