Security Assurance and Monitoring Procedure

Tarralea Digital Pty Ltd

Document ID	SEC-PRO-05
Version	1.6
Classification	PROTECTED
Document owner	Chief Information Security Officer
Approved by	Cyber Security Steering Committee
Effective date	1 April 2026
Next review	1 April 2027
Applies to	TARRALEA-PROTECTED

1. Purpose

This procedure sets out how Tarralea Digital Pty Ltd ("Tarralea") monitors the security of TARRALEA-PROTECTED and assures the effectiveness of its controls (GOV-03, DET-01). It supports the Information Security Policy (SEC-POL-01).

2. Security monitoring

2.1 The Security Operations team ensures that security-relevant event logs and configuration changes for TARRALEA-PROTECTED are centrally collected, protected against unauthorised modification or deletion, and retained for the period required by the system register (DET-01).

2.2 The Security Operations team analyses collected events in a timely manner to detect cyber security events (DET-02).

2.3 Where a security event meets the alerting criteria, the Security Operations team raises a cyber security incident and responds to it under the Cyber Security Incident Response Plan (SEC-PLN-03).

2.4 The Chief Information Security Officer reviews the coverage and effectiveness of security monitoring quarterly and directs improvements (DET-05).

3. Vulnerability reporting

3.1 The Security Operations team produces a monthly vulnerability report for TARRALEA-PROTECTED, drawn from the vulnerability scanning performed under the System Hardening and Configuration Management Standard (SEC-STD-04).

3.2 The Cyber Security Steering Committee reviews the monthly vulnerability report and prioritises the vulnerabilities identified in it.

4. Security assessment

4.1 An independent assessor conducts a security assessment of the platform controls for the TARRALEA-PROTECTED platform at least every twelve months, and following any significant change to the environment (ISM-1636).

4.2 During the security assessment, the assessor examines the configuration baseline register, reviews each recorded baseline deviation, and reviews each multi-factor authentication exception recorded under the Access Control and Identity Management Standard (SEC-STD-02).

4.3 The assessor produces a security assessment report that states the residual security risk for the TARRALEA-PROTECTED platform.

4.4 Following each security assessment, the Cyber Security Steering Committee reviews the security assessment report, accepts the residual security risk for the TARRALEA-PROTECTED platform, and approves the continued operation of the TARRALEA-PROTECTED platform.

5. Authorisation to operate

5.1 The Platform Owner maintains the authorisation to operate for TARRALEA-PROTECTED and initiates a reauthorisation whenever a significant change is made to the environment (ISM-0027).

5.2 The Chief Information Security Officer ensures that the system register records the current authorisation status of TARRALEA-PROTECTED.

6. Annual security status reporting

6.1 The Platform Owner produces an annual security status report for TARRALEA-PROTECTED covering its control status, outstanding vulnerabilities and open security risks, and files the report in the assurance register.

7. Continuous improvement

7.1 The Chief Information Security Officer ensures that lessons from monitoring, assessments and exercises are used to improve the controls for TARRALEA-PROTECTED, and reports improvement actions to the Cyber Security Steering Committee, which directs their implementation (GOV-07).

8. Records

Record	Maintained by	Consumed by
Monthly vulnerability report	Security Operations team	Cyber Security Steering Committee (clause 3.2)
Security assessment report	Independent assessor	Cyber Security Steering Committee (clause 4.4)
Annual security status report	Platform Owner	Assurance register (clause 6.1)

9. Review

The Chief Information Security Officer reviews this procedure at least annually.

Version history

Version	Date	Author	Summary
1.0	Jun 2024	CISO	Initial issue
1.3	Sep 2025	CISO	Added independent security assessment cadence
1.6	Apr 2026	CISO	Annual review; aligned to ISM GOV and DET principles