System Hardening and Configuration Management Standard

Tarralea Digital Pty Ltd

Document ID	SEC-STD-04
Version	2.2
Classification	PROTECTED
Document owner	Platform Owner
Approved by	Cyber Security Steering Committee
Effective date	1 April 2026
Next review	1 April 2027
Applies to	TARRALEA-PROTECTED

1. Purpose

This standard sets out the configuration and hardening requirements for TARRALEA-PROTECTED (PRO-04). It enacts the system hardening requirement of the Information Security Policy (SEC-POL-01, clause 6.1) and supports the secure system lifecycle (PRO-01).

2. Approved baselines

2.1 The Platform Owner establishes and maintains an approved hardening baseline for each operating system, server application and platform component used in TARRALEA-PROTECTED.

2.2 Each approved baseline applies vendor and ASD hardening guidance for the relevant component, disables unused functions, services and accounts, and restricts administrative interfaces to authorised management networks.

2.3 The Security Operations team configures every component of TARRALEA-PROTECTED to its approved baseline before the component enters service.

2.4 The Security Operations team records the approved baseline applied to each component, and the configuration of each component, in the configuration baseline register.

2.5 The Platform Owner records each approved baseline and each subsequent change to a baseline in the configuration baseline register, which is examined during the security assessment of TARRALEA-PROTECTED under the Security Assurance and Monitoring Procedure (SEC-PRO-05).

3. Baseline deviations

3.1 A deviation from an approved baseline may be permitted where a documented business justification and the compensating controls are recorded in the configuration baseline register.

3.2 A deviation from an approved baseline is reviewed at the next security assessment of TARRALEA-PROTECTED under the Security Assurance and Monitoring Procedure (SEC-PRO-05).

4. Software authorisation

4.1 TARRALEA-PROTECTED permits the execution of only software that is supported, verified and authorised (PRO-07).

4.2 The Platform Owner maintains the authorised software list for TARRALEA-PROTECTED.

4.3 The Security Operations team configures application control on TARRALEA-PROTECTED to permit the execution of software on the authorised software list and to prevent the execution of all other software.

5. Change management

5.1 The Platform Owner approves every change to the configuration of TARRALEA-PROTECTED before it is applied.

5.2 The Security Operations team applies approved changes and updates the configuration baseline register to reflect each applied change.

6. Vulnerability management

6.1 The Security Operations team identifies vulnerabilities in TARRALEA-PROTECTED through regular vulnerability scanning (PRO-06).

6.2 The Security Operations team remediates vulnerabilities identified on TARRALEA-PROTECTED that are rated High or above within the maximum remediation timeframes specified in the Security Assurance and Monitoring Procedure (SEC-PRO-05).

6.3 The Security Operations team validates that each remediation has been applied effectively.

7. Records

Record	Maintained by	Consumed by
Configuration baseline register	Platform Owner / Security Operations team	Security assessment (SEC-PRO-05)
Authorised software list	Platform Owner	Application control configuration (clause 4.3)

8. Review

The Platform Owner reviews this standard at least annually.

Version history

Version	Date	Author	Summary
1.0	May 2024	Platform Owner	Initial issue
2.0	Jul 2025	Platform Owner	Added application control requirements
2.2	Apr 2026	Platform Owner	Annual review; aligned to ISM PRO principles