Access Control and Identity Management Standard

Tarralea Digital Pty Ltd

Document ID	SEC-STD-02
Version	2.4
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 standard sets out the identity, credential and access management requirements for TARRALEA-PROTECTED (PRO-13). It supports the Information Security Policy (SEC-POL-01).

2. Account lifecycle

2.1 User accounts on TARRALEA-PROTECTED are created following the approval of an access request. The Platform Owner approves the creation of all user accounts on TARRALEA-PROTECTED.

2.2 The Security Operations team provisions each user account in accordance with the approved access request.

2.3 The Security Operations team disables a user account within one business day of being notified by People & Culture that the account holder has changed role or left Tarralea.

2.4 Personnel and services are granted the minimum access to TARRALEA-PROTECTED required to undertake their duties (PRO-12).

3. Privileged access

3.1 Privileged (administrator) access to TARRALEA-PROTECTED is granted only where it is required for a defined operational duty.

3.2 The Platform Owner approves all grants of privileged access to TARRALEA-PROTECTED.

3.3 The Security Operations team provisions privileged access in accordance with the approved request and applies the least-privilege principle to the access granted (PRO-12, PRO-05).

3.4 Privileged accounts are used only for administrative tasks. The Security Operations team ensures that holders of privileged accounts use a separate unprivileged account for all non-administrative activity.

3.5 The Chief Information Security Officer authorises the grant of privileged access to TARRALEA-PROTECTED.

3.6 All grants of privileged access to TARRALEA-PROTECTED are recorded in the privileged access register, which is maintained by the Security Operations team for audit purposes.

4. Multi-factor authentication

4.1 The Security Operations team enforces multi-factor authentication for all users of TARRALEA-PROTECTED (PRO-13).

4.2 Multi-factor authentication used for authenticating users of TARRALEA-PROTECTED is phishing-resistant (ISM-1682).

4.3 The Security Operations team ensures that successful and unsuccessful multi-factor authentication events are centrally logged (ISM-1683). The Security Operations team analyses these events as part of security monitoring under the Security Assurance and Monitoring Procedure (SEC-PRO-05).

4.4 Where a service account cannot support multi-factor authentication, an exception is recorded together with a documented business justification and the compensating controls applied. Each multi-factor authentication exception is reviewed at the next security assessment of TARRALEA-PROTECTED under the Security Assurance and Monitoring Procedure (SEC-PRO-05).

5. Passwords

5.1 Passwords used for multi-factor authentication on TARRALEA-PROTECTED are a minimum of 6 characters and are not reused across accounts (ISM-1559).

5.2 Passwords used for single-factor authentication on TARRALEA-PROTECTED, where multi-factor authentication cannot be supported, are a minimum of 4 random words (ISM-0421).

5.3 The Security Operations team configures TARRALEA-PROTECTED so that passwords appearing in lists of commonly used or compromised passwords cannot be set (ISM-2078), and so that the maximum password length is not less than 64 characters (ISM-2079).

6. Records

Record	Maintained by
Privileged access register	Security Operations team
Multi-factor authentication exception list	Security Operations team

7. Review

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

Version history

Version	Date	Author	Summary
1.0	Mar 2024	CISO	Initial issue
2.0	Apr 2025	CISO	Added phishing-resistant MFA requirement
2.3	Jan 2026	CISO	Updated password requirements per ISM
2.4	Apr 2026	CISO	Annual review