Cyber Security Incident Response Plan

Tarralea Digital Pty Ltd

Document ID	SEC-PLN-03
Version	4.0
Classification	PROTECTED
Document owner	Head of Security Operations
Approved by	Chief Information Security Officer
Effective date	1 April 2026
Next review	1 April 2027
Applies to	TARRALEA-PROTECTED

1. Purpose

This plan sets out how Tarralea Digital Pty Ltd ("Tarralea") prepares for, detects, responds to and recovers from cyber security incidents affecting TARRALEA-PROTECTED (RES-01, RES-05). It supports the Information Security Policy (SEC-POL-01).

2. Roles

2.1 The Head of Security Operations directs the response to every cyber security incident affecting TARRALEA-PROTECTED.

2.2 Once an incident has been declared Critical, the Chief Information Security Officer assumes decision authority for the response, and the Head of Security Operations continues to direct response operations under that authority.

2.3 The Security Operations team carries out detection, triage, containment, eradication and recovery activities.

3. Incident severity

3.1 Every cyber security incident is assigned a severity of Low, Moderate, High or Critical.

3.2 A cyber security incident is declared Critical when it meets any of the following criteria:

- confirmed unauthorised access to PROTECTED data held on TARRALEA-PROTECTED;
- loss of availability of a hosted agency workload exceeding four hours; or
- confirmed compromise of a privileged account on TARRALEA-PROTECTED.

3.3 The Head of Security Operations assigns the severity of Low, Moderate and High incidents.

4. Response process

4.1 **Detect and record.** On identifying a cyber security event, the Security Operations team analyses it to determine whether it constitutes a cyber security incident, and records each confirmed incident in the cyber security incident register (ISM-0125).

4.2 **Report internally.** The Security Operations team reports every confirmed cyber security incident to the Chief Information Security Officer, or one of their delegates (ISM-0123).

4.3 **Notify executive.** Where an incident is declared Critical, the Chief Information Security Officer notifies the Chief Executive Officer and the Chief Operating Officer without delay.

4.4 **Contain and recover.** The Security Operations team contains the incident, eradicates the cause, and restores affected agency workloads to normal operation.

4.5 **Close.** The Head of Security Operations closes the incident in the cyber security incident register once recovery is confirmed.

5. Incident register

5.1 The cyber security incident register contains, for each cyber security incident (ISM-1803):

- the date the incident occurred;
- the date the incident was discovered;
- a description of the incident;
- the severity assigned;
- the actions taken in response; and
- to whom the incident was reported.

5.2 The Head of Security Operations maintains the cyber security incident register. The Audit, Risk and Compliance Committee reviews incident trends drawn from the cyber security incident register at each meeting and directs any resulting remediation.

6. Post-incident review

6.1 Following every Critical incident, the Head of Security Operations conducts a post-incident review and produces a post-incident review report.

6.2 The Cyber Security Steering Committee reviews each post-incident review report and directs improvements to controls and to this plan arising from it (GOV-07).

7. Exercises

7.1 The Head of Security Operations exercises this plan at least annually and documents the outcomes (ISM-1784). The Cyber Security Steering Committee reviews the exercise outcomes and directs any required improvements.

8. Review

The Head of Security Operations reviews this plan at least annually and after every Critical incident.

Version history

Version	Date	Author	Summary
1.0	Mar 2024	HSO	Initial issue
2.0	Nov 2024	HSO	Added severity model
3.0	Aug 2025	HSO	Revised escalation and executive notification
4.0	Apr 2026	HSO	Annual review; aligned to ISM RES principles