Patch and Vulnerability Management Policy

Table of contents

Title	Patch and Vulnerability Management Policy
Doc#	POL-ITMA-031
Version	1.0
Date	24-03-2025
Supersedes	No prior issued policy; formalises the informally-referenced `vuln_mgmt` cited by the NIST control mapping
Next Review	24-03-2026
Owner	Head of IT (H. Boyd)
Approved By	Chief Information Officer (A. Vasquez)
ISO/IEC 27001:2022	A.8.8 Management of technical vulnerabilities

[Reviewer, 2025-03-19: this is the first formally issued version of this policy. The NIST control mapping (support/nist_mapping.md) already links a `vuln_mgmt` document at reference [18] that was never actually issued — this document closes that gap. Point any remaining references at this number rather than re-creating the placeholder.]

1. Purpose and scope

This policy sets out how Tessera manages technical vulnerabilities across its applications, operating systems, endpoints and cloud infrastructure, so that known weaknesses are patched or mitigated before they can be exploited. It gives effect to **APP 11** (security of personal information) of the *Privacy Act 1988* (Cth) and to Annex A control **A.8.8** (management of technical vulnerabilities) of ISO/IEC 27001:2022. It also maps directly to the ACSC Essential Eight mitigation strategies **"Patch applications"** and **"Patch operating systems"**.

The policy applies to all Tessera-managed assets in scope of the ISMS — workforce endpoints, servers, network devices, container images and the AWS workloads running the platform in `ap-southeast-2` (Sydney) and the declared standby in `ap-southeast-1` (Singapore) — and to the legacy IT footprint at the Malaga WA operations centre.

Timely patching after the breach **TSR-INC-2025-031** is a board-level expectation under Tessera's ISO/IEC 27001:2022 certification-readiness mandate.

2. Policy statements

Tessera policy requires that:

(a) all in-scope systems are kept at a supported and patched software and operating-system level;

(b) security patches for applications and operating systems are applied within **14 days** of a fix being released by the vendor;

(c) where a working exploit is known to exist for a vulnerability affecting an in-scope system, the patch or an effective mitigation is applied within **48 hours**;

(d) vulnerabilities are identified through regular authenticated scanning and through vendor and threat-intelligence advisories;

(e) unsupported or end-of-life software and operating systems are removed, isolated or replaced, and are not permitted in production;

(f) every asset in the inventory (POL-ITMA-009) has a defined patch owner and patch source;

(g) any deviation from the timeframes above is recorded as a formal exception under §3.4 with a compensating control and an expiry date.

3. Controls and procedures

3.1 Patch timeframes

1. Standard security patches for both applications and operating systems are deployed within **14 days** of release.
2. Where a working exploit is publicly known, or is being used in the wild, the remediation window shortens to **48 hours**.
3. Non-security functional updates follow the normal change process (POL-CHANGE-001) and are not governed by the security timeframes above.

3.2 Vulnerability scanning and coverage

1. Authenticated vulnerability scans are run across the in-scope estate on at least a **monthly** cadence, with the external attack surface scanned weekly.
2. Scan results are triaged by IT with Security oversight; findings are ranked by severity (CVSS) and exploitability and fed into the remediation queue.
3. Coverage is reconciled against the asset inventory so that no in-scope asset is left unscanned.

   [Reviewer, 2025-03-18: the monthly authenticated-scan cadence is stated here as policy, but I could not locate retained scan reports or a scan schedule for the last two quarters. Hamish confirms ad-hoc scans have been run but records are not being kept centrally — we cannot currently evidence this control for the Stage 1 audit. Open action for IT to stand up a retained scan register.]

3.3 Patch-compliance reporting

1. IT reports patch-compliance monthly to the CIO and to the ISMS forum.
2. Compliance is expressed as the percentage of in-scope assets patched within the applicable window.

   *[Reviewer, 2025-03-18: reported compliance sits in the "high-nineties percent" range, but the **denominator is not defined** — it is unclear whether the figure covers all in-scope endpoints or only the centrally-managed (Intune) estate. Bring-your-own and the Malaga legacy machines may be excluded from the count, which would materially overstate coverage. This must be pinned down and the denominator published before the number can be relied upon.]*

3.4 Legacy and unsupported software

1. Unsupported operating systems and applications are removed from production or placed behind a documented, time-boxed compensating control.
2. The **Malaga WA legacy footprint** is acknowledged as harder to patch and monitor than the rest of the estate and is treated as elevated risk until decommissioned.

   *[Reviewer, 2025-03-19: a decommission plan for the Malaga legacy footprint has been **requested but not yet approved**. Until it is funded and scheduled, these hosts remain a standing exception to §2(b)/(e) with no firm end date — flag to the risk register (POL-RISK-001) and to the CIO.]*

3.5 Exception handling

1. Any system that cannot meet the patch timeframes requires a formal exception approved by the Head of IT and reviewed by the CISO.
2. Each exception records the affected asset, the reason, the compensating control, the residual-risk rating and an expiry date.
3. Exceptions are reviewed at least quarterly and closed as soon as the underlying constraint is resolved.

Document status: v1.0, issued 24-03-2025. Next scheduled review: 24-03-2026. Questions about this policy go to `itsupport@tessera.locoensayo.org`.