User Application Hardening Standard

Table of contents

Title	User Application Hardening Standard
Doc#	SEC-STD-012
Version	1.0
Date	28-03-2025
Supersedes	None — new standard
Next Review	28-03-2026
Owner	Head of IT (H. Boyd), SOE / endpoint function
Approved By	Chief Information Security Officer (I. Ferreira)
ISO/IEC 27001:2022	A.8.9 Configuration management

[Reviewer, 2025-03-27: paired with SEC-STD-011 (Office Macro Configuration) under the SOE/endpoint function. Both standards give effect to the Essential Eight hardening pillars that Tessera's readiness assessment flagged as lacking a controlling document.]

1. Purpose and scope

This standard defines the mandatory hardening baseline for user applications and the standard operating environment (SOE) on Tessera-managed endpoints. Reducing the features and content that everyday applications will execute shrinks the attack surface available to malicious

web content and documents. The standard gives effect to **APP 11** (security of personal information) of the *Privacy Act 1988* (Cth) and to Annex A control **A.8.9** (configuration management) of ISO/IEC 27001:2022, and implements the ACSC Essential Eight mitigation strategy **"User application hardening"**.

It applies to every Tessera-managed device (Perth HQ, Sydney, and the Malaga WA operations centre) and to any bring-your-own device enrolled for Tessera or tenant work.

2. Policy statements

Tessera policy requires that:

(a) all Tessera-managed endpoints are built from a defined, version-controlled **standard operating environment (SOE) baseline**;

(b) web browsers are hardened to **block Flash content, Java, and web advertisements**, and to disable features that are not needed for business use;

(c) PDF readers are hardened — JavaScript in documents is disabled and protected/sandboxed viewing modes are enabled;

(d) unneeded operating-system features, components and services are disabled or removed from the baseline;

(e) the hardened configuration is **enforced centrally** and cannot be relaxed by the user;

(f) any deviation from the baseline is handled through the exception process in §3.4.

3. Controls and procedures

3.1 Standard operating environment baseline

1. IT maintains a documented SOE baseline for each supported platform, held under version control.
2. New devices are provisioned from the baseline; drift is expected to be detected and corrected by configuration management.

3.2 Browser hardening

1. Adobe Flash Player is removed; where a runtime is present it is blocked.
2. Java in the browser is disabled unless a documented line-of-business need exists.
3. Web advertisements are blocked at the browser and/or network layer.
4. Unneeded browser features are disabled in the baseline profile.

3.3 PDF-reader and OS hardening

1. The approved PDF reader is configured with document JavaScript disabled and protected view enabled.
2. Unneeded Windows/macOS components and services are disabled or removed from the SOE.

3.4 Exceptions

1. Deviations from the baseline require a formal, time-boxed exception approved by the Head of IT and reviewed by the CISO, with a compensating control and an expiry date.
2. Legacy line-of-business applications that cannot run under the hardened baseline are recorded as standing exceptions with a remediation or replacement plan.

   *[Reviewer, 2025-03-27: the hardened baseline in §3.1–§3.3 is **documented but never evidenced as enforced**. There is no configuration-compliance report showing that live endpoints actually match the SOE — so we cannot demonstrate the control is operating, only that it is written down. This is the same evidencing gap as SEC-STD-011; a single compliance-reporting mechanism should cover both. Open action for the SOE function ahead of Stage 1.]*

   *[Reviewer, 2025-03-27: two carve-outs weaken the baseline in practice — **browser extensions are permitted by exception** (with no central allow-list evidenced), and several **legacy line-of-business apps require carve-outs**, concentrated on the Malaga legacy footprint which is harder to bring under the managed SOE. Neither carries a firm remediation date. Reconcile with the patch/vulnerability position (POL-ITMA-031) and the risk register.]*

Document status: v1.0, issued 28-03-2025. Next scheduled review: 28-03-2026. Questions about this standard go to `itsupport@tessera.locoensayo.org`.