Microsoft Office Macro Configuration Standard

Table of contents

Title	Microsoft Office Macro Configuration Standard
Doc#	SEC-STD-011
Version	1.0
Date	26-03-2025
Supersedes	None — new standard
Next Review	26-03-2026
Owner	Head of IT (H. Boyd), SOE / endpoint function
Approved By	Chief Information Security Officer (I. Ferreira)
ISO/IEC 27001:2022	A.8.19 Installation of software on operational systems

[Reviewer, 2025-03-24: this standard is referenced by the Essential Eight readiness tracker but had no controlling document until now. It sits under the SOE/endpoint function alongside SEC-STD-012 (User Application Hardening).]

1. Purpose and scope

This standard defines the mandatory configuration for Microsoft Office macro settings on all Tessera-managed endpoints. Malicious macros are a well-known delivery mechanism for malware and credential theft; constraining how macros execute reduces that attack surface. The standard

gives effect to **APP 11** (security of personal information) of the *Privacy Act 1988* (Cth) and to Annex A control **A.8.19** (installation of software on operational systems) of ISO/IEC 27001:2022, and implements the ACSC Essential Eight mitigation strategy **"Configure Microsoft Office macro settings"**.

It applies to every Tessera-managed device running Microsoft Office (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) macros are **disabled by default** in all Microsoft Office applications on Tessera-managed endpoints;

(b) only macros that are **digitally signed by a trusted publisher** and run from a **trusted location** are permitted to execute;

(c) macros in files that originate from the **internet** (carrying the mark-of-the-web) are **blocked** and cannot be enabled by the user;

(d) users cannot enable macros or alter macro security settings themselves — settings are enforced centrally and locked;

(e) macro execution is **logged** and the logs are retained and available to Security;

(f) any requirement to run unsigned or third-party macros is handled only through the exception process in §3.4.

3. Controls and procedures

3.1 Baseline configuration

1. In Word, Excel, PowerPoint, Outlook, Access and Visio, the macro setting is configured to **"Disable all except digitally signed macros"**.
2. Trusted locations are restricted to a small, defined set of IT-controlled paths; users cannot add trusted locations.
3. The list of trusted publishers is centrally managed; a publisher certificate is added only after Security review.

3.2 Blocking macros from the internet

1. The "Block macros from running in Office files from the Internet" setting is enabled fleet-wide.
2. Files carrying the mark-of-the-web present a hard block, not a dismissible "Enable content" prompt.

3.3 Logging

1. Macro execution and blocked-macro events are logged locally and forwarded to the central logging pipeline.
2. Security reviews anomalous macro activity as part of routine monitoring.

3.4 Exceptions

1. Any need to run unsigned macros requires 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. A standing exception currently permits **Finance's legacy spreadsheet templates** to run **unsigned** macros from a shared network location.

   [Reviewer, 2025-03-24: the Finance carve-out is a material weakening of this standard. It permits unsigned macros from a shared location that multiple users can write to, which is exactly the vector §2 is meant to close. It has no expiry date and no compensating control recorded. This needs a remediation plan (re-sign the templates under a trusted publisher, or migrate them off macros) before the Stage 1 audit.]

   [Reviewer, 2025-03-25: more fundamentally, I can find ***no evidence of central GPO/Intune enforcement*** *of the settings in §3.1–§3.2. The baseline is asserted in this document but is not demonstrably pushed to, or locked on, the fleet — especially the Malaga legacy machines, which are outside the main Intune ring. Without a configuration-compliance report this control cannot be evidenced as operating. Open action for the SOE function.]*

Document status: v1.0, issued 26-03-2025. Next scheduled review: 26-03-2026. Questions about this standard go to `itsupport@tessera.locoensayo.org`.