Southern Mutual Bank

Office Macro Configuration Export — Microsoft 365 Tenant

configuration export · settings read from the system of record · synthetic assessor-grade test document

Export ID	SOU-EXP-1225
System	Microsoft 365 Tenant
Exported by	Aisha Khan (Security Operations Lead)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Microsoft 365 Tenant: the current settings as held by the system, section by section, with the compliance status against the applicable baseline. It reports state; it does not describe intent. Settings shown as non-compliant carry a remediation ticket.

2. Microsoft Office macro settings (tenant policy)

Setting	Value	Status
Macros in files from the internet	Blocked — cannot be enabled by users; Mark of the Web enforced	Compliant
Macros for users without a demonstrated business requirement	Blocked — macro execution off for 1,102 of 1,244 users	Compliant
Macros permitted	Only digitally signed macros from trusted publishers, for the 142 users in the finance and treasury macro group	Compliant
Trusted publishers list	Managed centrally — 3 publishers; users cannot add publishers	Compliant
Macro antivirus scanning	Antivirus scanning of macros enabled (AMSI) — malware and malicious code scanned before execution	Compliant
Win32 API calls from macros	Blocked by attack surface reduction rule	Compliant
Users can change macro security settings	No — settings locked by tenant policy	Compliant
Macro security policy — Excel 4.0 (XLM) macros	Blocked	Compliant

3. Attack surface reduction rules (macro-related, hardening)

Setting	Value	Status
Block Office applications from creating child processes	Block mode	Compliant
Block Office applications from creating executable content	Block mode	Compliant
Block Office applications from injecting code into other processes	Block mode	Compliant
Block execution of potentially obfuscated scripts	Block mode	Compliant

Setting	Value	Status
Macro execution events logged	Blocked and allowed macro executions logged and forwarded to the SIEM	Compliant

4. Control framework mapping

Framework	Indicative mapped controls
APRA CPS 234	Information security capability, Control testing, Incident notification
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2

Exported from the management console; integrity hash recorded in the evidence register. Reviewed by the control owner and second-line risk.