Southern Mutual Bank

Browser and PDF Reader Hardening Configuration Export — Workstations

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

Export ID	SOU-EXP-1226
System	Workstations
Exported by	Laura Mendez (Third-Party Risk Manager)
Exported	09 Nov 2026 00:00
Source	management console / configuration management database
Status	Complete

1. What this export is

A configuration export for Workstations: 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. Web browser hardening (user application hardening baseline)

Setting	Value	Status
Java from the internet	Blocked — web browsers do not process Java from the internet	Compliant
Web advertisements from the internet	Blocked — ad blocking extension enforced; web browsers do not process web advertisements	Compliant
Internet Explorer 11	Removed — not available to users	Compliant
Browser security settings	Hardened per the ASD hardening guidance; users cannot change security settings	Compliant
Browser extensions	Allowlisted extensions only — 6 approved	Compliant
SmartScreen / Safe Browsing	Enforced — malicious site and download blocking	Compliant
Browser telemetry to the SIEM	Security events forwarded	Compliant

3. PDF reader and Office hardening

Setting	Value	Status
PDF reader — JavaScript	Blocked	Compliant
PDF reader — protected mode / sandbox	Enforced	Compliant
PDF reader — embedded content and external links	Blocked from executing automatically	Compliant
Microsoft Office — object linking and embedding packages	Blocked	Compliant
Microsoft Office — child process creation and Flash content	Blocked	Compliant
PowerShell	Constrained language mode; script block logging and module logging enabled; logs forwarded to the SIEM	Compliant
Windows Script Host and .NET Framework 3.5	Blocked / removed	Compliant

Setting	Value	Status
Hardening baseline compliance	1242 of 1,244 workstations compliant; drifted devices remediated by policy re-apply	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.