Microsoft Intune Attack Surface Reduction (ASR) Policy — ISO 27001 Aligned

Role: Security Operations (SOC) Analyst – Lab Project

Tools: Microsoft Intune, Microsoft Defender for Endpoint, Microsoft Defender for Cloud, Azure Active Directory

Frameworks: ISO/IEC 27001:2022, Microsoft Secure Score

Project Summary

Configured and deployed Microsoft Intune Attack Surface Reduction (ASR) rules to strengthen endpoint security posture and increase Microsoft Defender Secure Score. The implementation directly addressed top security recommendations and aligned with ISO/IEC 27001:2022 control objectives.

Objectives

- Record baseline Microsoft Defender Secure Score from Microsoft Defender for Cloud.

- Configure and deploy ASR rules via Intune to address high-priority gaps.

- Validate policy deployment and confirm Secure Score improvement.

- Map ASR configurations to ISO 27001 Annex A controls for compliance reporting.

Scope

- Applied targeted ASR rules to block malware delivery methods, including USB, email attachments, Office macros, and script-based attacks.
- Mapped changes to ISO/IEC 27001:2022 controls for monitoring, logging, and access management.
- Verified Secure Score improvements post-implementation.

Implementation Steps

1. Recorded baseline Secure Score from Microsoft Defender for Cloud.

2. Configured ASR rules in Microsoft Intune for endpoint protection.

3. Applied policies targeting high-priority security gaps identified in Secure Score.

4. Validated deployment success in Intune compliance dashboard.

5. Recorded post-implementation Secure Score to measure improvement.

6. Mapped ASR rule coverage to ISO/IEC 27001 Annex A controls.

ISO/IEC 27001:2022 Control Mapping

Control	Goal	Coverage
A.8.15 – Logging	Ensure security-relevant events are recorded.	Defender and Intune generate logs for policy changes and enforcement.
A.8.16 – Monitoring Activities	Continuously monitor security controls.	Secure Score dashboard tracks security posture changes in real time.
A.5.15 – Access Control	Restrict and manage system access.	ASR rules limit execution of potentially malicious files and scripts.

Results & Impact

- Increased Secure Score from 44.4% to 46.22%.

- Blocked malware delivery vectors including USB, email, Office macros, and script-based threats.

- Reduced attack surface against ransomware and phishing campaigns.

Key Skills Demonstrated

- Endpoint hardening and policy configuration in Microsoft Intune.

- Security posture improvement and measurement using Microsoft Secure Score.

- Compliance mapping to ISO/IEC 27001:2022.

- Integration of endpoint protection with Microsoft Defender for Endpoint.