					Insert Registered Legal Entity Name Here							
Document number: P20					Document Title: **Endpoint Protection / Malware Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Endpoint protection and malware controls are required to meet ISMS objectives
ISO/IEC 27002:2022	Controls 8.7, 8	Provides technical controls and guidance for anti-malware, endpoint defense, and incident management
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Defines malicious code protection, centralized monitoring, and configuration baseline requirements
EU GDPR	Article 32	Requires appropriate technical measures to safeguard personal data, including protection against malware
EU NIS2	Article 21(2)(d)	Requires deployment of endpoint-level threat detection and preventive measures
EU DORA	Article 9	Requires ICT risk management for malware and endpoint-borne threat defense
COBIT 2019	DSS05.01, DSS01.04, MEA	Requires protection, monitoring, and assessment of endpoint controls

1. Purpose

1.1 This policy defines the mandatory controls and operational requirements for protecting organizational endpoints—including desktops, laptops, mobile devices, and servers—from malware and related threats.

1.2 It establishes minimum standards for endpoint protection, malware detection, containment, response, and behavioral monitoring, ensuring that systems remain resilient against both commodity and advanced malware strains.

1.3 This policy directly supports compliance with ISO/IEC 27001:2022 Clause 8.1 and Annex A Control 8.7 and is aligned with regional cybersecurity obligations under GDPR, NIS2, and DORA.

2. Scope

2.1 This policy applies to all endpoints, including:

2.1.1 Organization-owned or organization-managed desktops, laptops, mobile devices, and virtual instances

2.1.2 Personally owned devices authorized under the BYOD policy, subject to MDM or endpoint agent installation

2.1.3 Servers and infrastructure assets, including cloud-hosted VMs and edge devices

2.1.4 Operating systems, drivers, local services, endpoint agents, and security controls installed on each node

2.2 All personnel with administrative, technical, or operational responsibility for any endpoint are subject to this policy, including:

2.2.1 Internal employees, contractors, and third-party service providers

2.2.2 Managed service providers (MSPs), outsourced desktop support providers, and third-party IT administrators

2.2.3 Users authorized to operate portable systems, corporate VPN-enabled laptops, or mobile access to organizational networks

2.3 Threats covered under this policy include, but are not limited to:

2.3.1 Viruses, worms, trojans, ransomware, spyware, rootkits, adware, keyloggers, and botnets

2.3.2 Fileless malware, zero-day payloads, privilege escalation malware, and browser exploit kits

2.3.3 Malicious code delivered via removable media, phishing vectors, drive-by downloads, or USB-based attacks

3. Objectives

3.1 Protect the integrity, availability, and confidentiality of endpoint systems and the data they process through effective malware prevention, detection, and response.

3.2 Prevent the execution or propagation of malicious code on organizational networks by enforcing technical controls, baseline hardening, and real-time telemetry.

3.3 Integrate endpoint protection with other Information Security Management System (ISMS) controls, including vulnerability management, access control, the Logging and Monitoring Policy, and incident response.

3.4 Ensure continuous endpoint visibility through centrally managed protection platforms, including antivirus/anti-malware agents, EDR (Endpoint Detection and Response), and SIEM telemetry.

3.5 Comply with legal, regulatory, and standards-based requirements mandating endpoint security (e.g., GDPR Article 32, NIS2 Article 21, DORA Article 9).

3.6 Define accountable roles, enforce patching and alert response notification service level agreements, and enable audit readiness through documentation and reporting.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures its alignment with the Information Security Management System (ISMS) and overall security strategy.

4.1.2 Reviews endpoint protection metrics, incident trends, and tool effectiveness quarterly.

4.1.3 Approves exceptions and residual risk acceptances related to endpoint coverage.

4.2 Endpoint Security Lead / SOC Manager

4.2.1 Manages endpoint protection systems (e.g., AV, EDR, MDM).

4.2.2 Oversees policy enforcement, threat detection tuning, and response playbooks.

4.2.3 Maintains coverage statistics, malware incident logs, and alert configuration baselines.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy must be reviewed annually or when:

9.1.1 Major malware campaigns or endpoint security incidents occur

9.1.2 New threat types (e.g., fileless malware or ransomware variants) require updated detection or response strategies

9.1.3 Endpoint protection platforms or agent architectures change significantly

9.1.4 Legal or regulatory requirements affecting endpoint controls are updated

9.2 The review must be initiated by the Endpoint Security Lead and coordinated with the CISO, Legal and Compliance, Risk, and Audit and Compliance functions.

9.3 Approved revisions must be documented in the ISMS Document Control Register, assigned a new version identifier, and communicated to all affected parties.

9.4 Superseded versions must be archived, access-restricted, and retained for audit trail integrity in accordance with Information Security Management System (ISMS) retention schedules.

10. Related Policies and Linkages

10.1 P1 - Information Security Policy. Establishes foundational principles for the protection of systems, data, and networks. This policy enforces those principles at the endpoint level through technical and procedural malware controls.

10.2 P4 - Access Control Policy. Defines user access restrictions that are enforced at the endpoint layer, including protections against privilege escalation and unauthorized installation of unapproved software.

10.3 P5 - Change Management Policy. Ensures that updates to endpoint protection software, policy rules, or agent configurations are subject to approval and controlled deployment processes.

10.4 P12 - Asset Management Policy. Provides the asset classification and inventory baseline required for endpoint visibility, patch coverage, and definition of malware protection scope.

10.5 P22 - Logging and Monitoring Policy. Enables integration of endpoint alerts, agent health status, and threat intelligence into centralized SIEM systems for real-time detection and forensic traceability.

10.6 P30 - Incident Response Policy. Links endpoint-based malware incidents to standardized containment, eradication, investigation, and recovery workflows with assigned roles and escalation thresholds.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

11.1.1 Clause 8.1 - Operational Planning and Control: Requires implementation of technical controls, including endpoint safeguards, to maintain Information Security Management System (ISMS) objectives.

11.2 ISO/IEC 27002:2022 - Controls 8.7, 8:

11.2.1 Provides detailed technical guidance on anti-malware measures, secure software deployment, monitoring, and incident readiness for endpoint environments.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Malicious Code Protection: Requires the use of anti-malware tools with real-time, on-access scanning and behavioral analysis.

11.3.2 SI-4 - System Monitoring: Supports telemetry integration with centralized detection platforms.

11.3.3 CM-6 - Configuration Settings: Reinforces baseline control settings on endpoints, including enforcement of protection agents.

11.4 EU GDPR (2016/679):

11.4.1 Article 32 - Security of Processing: Requires organizations to implement appropriate technical measures to safeguard personal data, including protection against malware threats.

11.5 EU NIS2 Directive (2022/2555):

11.5.1 Article 21(2)(d): Requires entities to deploy threat detection and prevention measures, including malware defense mechanisms at the endpoint level.

11.6 EU DORA (2022/2554):

11.6.1 Article 9 - ICT Risk Management Requirements: Requires financial entities to adopt protective measures to prevent, detect, and respond to malware and endpoint-borne threats.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protect Against Malware: Requires detection and mitigation of malware across all organizational endpoints.

11.7.2 DSS01.04 - Manage Availability and Capacity: Ensures malware protection is balanced with system performance and business continuity.

11.7.3 MEA03 - Monitor, Evaluate and Assess Compliance: Requires periodic audit of endpoint controls and protection effectiveness.