					[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 where applicable

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 8.7, 8.23	
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(d)	
EU DORA	Article 9	
COBIT 2019	DSS05.01, DSS01.04, MEA03	

					[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

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 The 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 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 covered under this policy, including:

2.2.1 Internal employees and contractors

2.2.2 Managed Service Providers (MSPs), outsourced desktop support, and third-party IT administrators

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

2.3 Threat coverage under this policy includes, but is not limited to:

2.3.1 Viruses, worms, trojans, ransomware, spyware, rootkits, adware, keyloggers, 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 reliable malware prevention, detection, and response.

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

3.3 Integrate endpoint protection with other ISMS controls including vulnerability management, access control, logging and monitoring, 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 standard-based requirements mandating endpoint security (e.g., GDPR Article 32, NIS2 Article 21, DORA Article 9).

3.6 Define accountable roles, enforce patch and alert response SLAs, 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 ISMS and overall security strategy.

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

[.....]

11. Reference Standards and Frameworks

This policy is aligned with global cybersecurity standards and regulatory requirements for endpoint security, malware defense, and operational resilience.

ISO/IEC 27001:2022

Clause 8.1 - Operational Planning and Control: Requires the implementation of technical controls, including endpoint safeguards, to maintain ISMS objectives.

ISO/IEC 27002:2022 - Controls 8.7, 8.23

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

NIST SP 800-53 Rev.5

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

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

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

EU GDPR (2016/679)

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

COBIT 2019

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

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

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