					Insert Registered Legal Entity Name Here							
Document number: P20S					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	Operational controls for malware protection
ISO/IEC 27002:2022	Control 8	Control measures for endpoint protection
NIST SP 800-53 Rev.5	SI-3, SI-4	Malicious code protection and incident response
EU NIS2	Articles 21(2)(d), (e)	Malware and risk management for essential and important entities
EU DORA	Articles 10(1), 15	Operational resilience and third-party verification
COBIT 2019	DSS05.02, DSS05.04	Endpoint and network protection and monitoring
EU GDPR	Articles 32(1)(b), 33	Technical and organizational measures and breach notification

1. Purpose

1.1 This policy defines the minimum technical, procedural, and behavioral requirements for protecting all endpoint devices—such as laptops, desktops, mobile devices, and portable media—from malicious code, including viruses, ransomware, spyware, rootkits, and other malware threats.

1.2 Its purpose is to ensure that endpoints are equipped, maintained, and used in a manner that reduces the risk of malware infection, propagation, and system compromise.

1.3 The organization recognizes that endpoints are common malware entry points and must therefore be hardened, monitored, and protected using defense-in-depth strategies.

1.4 This policy supports the organization's ISO/IEC 27001:2022 certification objectives and aligns with the EU General Data Protection Regulation (GDPR), the NIS2 Directive, the Digital Operational Resilience Act (DORA), and other relevant frameworks.

2. Scope

2.1 This policy applies to:

2.1.1 All organizational endpoints, including desktops, laptops, tablets, mobile phones, and point-of-sale terminals

2.1.2 Personally owned (BYOD) devices used to access business applications or data

2.1.3 Removable storage devices such as USB drives and external hard disks

2.1.4 Any operating systems, endpoint software, or communication tools running on these platforms

2.2 It applies equally to:

2.2.1 Internal staff, contractors, interns, and managed service providers (MSPs)

2.2.2 Devices used on-site, remotely, or under hybrid work arrangements

2.2.3 Cloud-connected or offline endpoints storing business or personal data

3. Objectives

3.1 Prevent malware infection and propagation across internal systems, user devices, and external connections

3.2 Detect and contain malware-related threats promptly using automated endpoint security technologies and defined escalation paths

3.3 Ensure that only authorized, secured, and monitored devices are used to access business information

3.4 Enforce clear staff responsibilities and user behavior requirements to reduce the risk of malware-related incidents

3.5 Maintain traceable and auditable records of malware detections, responses, and policy compliance

3.6 Protect personal and business data from malware-related compromise using defense-in-depth strategies

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Owns this policy and ensures that sufficient resources are available for endpoint protection

4.1.2 Approves antivirus software, mobile device management (MDM) tools, and third-party access rules

4.1.3 Reviews malware incident reports, impact summaries, and data breach notifications involving endpoints

4.2 IT Support Provider / Internal IT Administrator

4.2.1 Selects and deploys antivirus, antimalware, and endpoint detection and response (EDR) software

4.2.2 Ensures that updates are applied consistently and logs are retained

4.2.3 Responds to malware alerts, isolates infected systems, and performs remediation

4.2.4 Enforces controls over USB and external device use

[... 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 Annual Review Requirement

9.1.1 This policy must be formally reviewed at least once per year by the General Manager, in coordination with the IT Support Provider and Privacy Coordinator

9.2 Trigger-Based Updates

9.2.1 This policy must also be updated when:

9.2.1.1 A significant new malware threat or outbreak targets endpoints used by the organization

9.2.1.2 Antivirus or EDR tools are changed, upgraded, or replaced

9.2.1.3 A malware incident reveals weaknesses in the scope or enforcement of this policy

9.2.1.4 Legal or regulatory requirements (e.g., GDPR, DORA, NIS2) are updated

9.3 Version Control and Communication

9.3.1 All policy changes must be documented with a version number, date, and summary of changes

9.3.2 Staff must be notified of updates, especially where they affect operational or behavioral requirements

9.3.3 Prior versions must be retained in the policy archive for at least 3 years to support audits

10. Related Policies and Linkages

10.1 This policy must be implemented in conjunction with the following SME policies:

10.1.1 P9S - Remote Work Policy: Ensures endpoint protection requirements are enforced on devices used off-site or in hybrid work settings

10.1.2 P12S - Asset Management Policy: Supports the tracking and control of all endpoints, ensuring that only authorized and protected devices are used

10.1.3 P17S - Data Protection and Privacy Policy: Reinforces malware prevention as a core privacy control to protect personal and sensitive data from compromise

10.1.4 P22S - Logging and Monitoring Policy: Establishes requirements for logging malware events and maintaining alert visibility to support early response

10.1.5 P30S - Incident Response Policy: Defines escalation, containment, and external notification steps if malware leads to data compromise or operational disruption

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 - Requires the implementation of operational controls to reduce risks such as malware attacks

11.2 ISO/IEC 27002

11.2.1 Control 8.7 - Details malware control practices, including antivirus, real-time scanning, updates, and user training

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 - Requires the deployment of malicious code protection mechanisms across endpoints

11.3.2 SI-4 - Requires monitoring, detection, analysis, and response actions for endpoint-level threats and alerts

11.4 EU GDPR

11.4.1 Article 32(1)(b) - Requires technical and organizational controls (such as antivirus) to protect personal data

11.4.2 Article 33 - Requires breach notification when malware compromises data integrity, confidentiality, or availability

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(d) - Requires measures to prevent and respond to malware threats within essential and important entities

11.5.2 Article 21(2)(e) - Requires layered cybersecurity risk management strategies, including endpoint malware protection

11.6 EU DORA

11.6.1 Article 10(1) - Requires ICT systems to be protected from malware and other threats as part of operational resilience

11.6.2 Article 15 - Requires financial entities to verify malware protection across third-party service providers

11.7 COBIT 2019

11.7.1 DSS05.02 - Emphasizes protective measures to defend endpoints and networks from malware threats

11.7.2 DSS05.04 - Supports monitoring and alerting for malware-related security events as part of ongoing operations