<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P20S</td><td colspan="7">Document Title:
<b>Endpoint Protection - Malware Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

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	Control 8.7	
NIST SP 800-53 Rev.5	SI-3, SI-4	
EU NIS2	Articles 21(2)(d), (e)	
EU DORA	Articles 10(1), 15	
COBIT 2019	DSS05.02, DSS05.04	
EU GDPR	Articles 32(1)(b), 33	

				[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

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 endpoints are equipped, maintained, and used in ways that reduce 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 multiple layers of defense.

1.4. The 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 communications tools running on these platforms

2.2. It applies equally to:

2.2.1. Internal staff, contractors, interns, and managed service providers

2.2.2. Devices used on-site, remotely, or via 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 quickly using automated endpoint security technologies and defined escalation paths

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

3.4. Enforce clear staff responsibilities and user behavior rules 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 compromise due to malware using defense-in-depth strategies

4. Roles and Responsibilities

4.1. **General Manager (GM)**

4.1.1. Owns this policy and ensures 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 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 updates are applied consistently and logs are retained

4.2.3. Responds to malware alerts, isolates infected systems, and conducts remediation
4.2.4. Enforces controls over USB and external device use

4.3. **Privacy Coordinator / Data Protection Lead**
4.3.1. Assesses whether malware-related incidents result in a data breach (per GDPR or DORA)
4.3.2.

[……..]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires implementation of operational controls to reduce risks such as malware attacks.

ISO/IEC 27002:2022

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

NIST SP 800-53 Rev.5

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

SI-4 – Mandates monitoring, detection, analysis, and response actions for endpoint-level threats and alerts.

EU GDPR

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

Article 33 – Obligates breach notification when malware compromises data integrity, confidentiality, or availability.

EU NIS2 Directive

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

Article 21(2)(e) – Mandates layered cybersecurity risk management strategies including endpoint malware protection.

EU DORA

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

Article 15 – Obligates financial organizations to verify malware protection across third-party service providers.

COBIT 2019

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

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