					[Insert Registered Legal Entity Name Here]							
Document number: P19S					Document Title: **Vulnerability and Patch Management 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 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Articles 21(2)(d), 21(2)(e)	
EU DORA	Articles 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12.01	
EU GDPR	Article 32(1)(b)	

					[Insert Registered Legal Entity Name Here]								
Document number: P19S					Document Title: **Vulnerability and Patch Management 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 how the organization identifies, evaluates, and mitigates vulnerabilities across systems, applications, and infrastructure.
   1.2. Its purpose is to reduce cybersecurity risk by enforcing timely patching and risk-based remediation practices suitable for small and mid-sized enterprises (SMEs).
   1.3. This policy supports compliance with ISO/IEC 27001:2022 certification and helps meet regulatory obligations under GDPR, NIS2, and DORA by requiring the proactive management of technical vulnerabilities.
   1.4. The organization recognizes that unpatched systems pose a significant threat to information security and must be addressed systematically and without delay.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All servers, desktops, laptops, mobile devices, network hardware, and cloud-hosted platforms used by the organization
      2.1.2. All operating systems, third-party software, plugins, and applications used in business operations
      2.1.3. Internal IT staff or external service providers responsible for system maintenance, updates, or monitoring
      2.1.4. Any custom-developed code or embedded software maintained by the organization or on its behalf
   2.2. The policy covers both infrastructure managed directly by the organization and systems administered by contracted vendors or hosting providers.
3. **Objectives**
   3.1. Identify and assess known vulnerabilities across all IT assets in a timely and consistent manner
   3.2. Apply patches and software updates based on severity and risk to organizational operations or personal data
   3.3. Prevent exploitation of technical weaknesses that could lead to service disruption, data breach, or legal noncompliance
   3.4. Maintain accurate records of applied patches, outstanding issues, and exceptions to ensure audit readiness
   3.5. Use tools and processes appropriate to the organization's size and operational complexity without compromising effectiveness
   3.6. Support legal and regulatory compliance, including GDPR Article 32 and ISO Annex A Control 8.8
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Holds overall responsibility for ensuring patching and vulnerability management activities are enforced
      4.1.2. Approves risk exceptions where patches cannot be applied and reviews related mitigation strategies

[…….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires implementation of controls to address operational risk, including vulnerability management.

ISO/IEC 27002:2022

Control 8.8 – Specifies processes for scanning and fixing known weaknesses in systems.

Control 8.9 – Emphasizes secure configuration, patch validation, and change control to avoid new exposures during updates.

NIST SP 800-53 Rev.5

RA-5 – Requires identification of vulnerabilities and remediation within defined timelines.

SI-2 – Mandates prompt application of patches and updates based on severity.

CM-2 – Governs system baseline configurations and update documentation to ensure consistent protections.

EU GDPR

Article 32(1)(b) – Requires organizations to implement appropriate technical measures, including patching, to maintain security of processing.

EU NIS2 Directive

Article 21(2)(d) – Requires handling of vulnerabilities through systematic scanning and remediation.

Article 21(2)(e) – Obligates secure configuration and patch management to ensure ICT resilience.

EU DORA

Article 8(1) – Requires detection and mitigation of ICT risks, including technical vulnerabilities.

Article 10(2) – Mandates financial entities to remediate weaknesses affecting ICT systems and operations.

COBIT 2019

DSS05.02 – Requires treatment of known technical vulnerabilities to maintain secure operations.

APO12.01 – Aligns risk management with proactive monitoring and correction of system weaknesses.