					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	
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	
EU GDPR	Article 32(1)(b)	

1. Purpose

1.1 This policy defines how the organization identifies, assesses, and remediates vulnerabilities across systems, applications, and IT infrastructure.

1.2 Its purpose is to reduce cybersecurity risk by enforcing timely patching and risk-based remediation practices appropriate for small and medium-sized enterprises (SMEs).

1.3 This policy supports compliance with ISO/IEC 27001:2022 certification requirements and helps meet regulatory obligations under the 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 personnel or external IT service providers responsible for system maintenance, updates, or monitoring and threat detection

2.1.4 Any custom-developed code or embedded code maintained by the organization or on its behalf

2.2 This policy covers both IT 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 personally identifiable information (PII)

3.3 Prevent exploitation of technical weaknesses that could lead to service outages, data breaches, or legal non-compliance

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

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Has overall responsibility for ensuring that patching and vulnerability management activities are enforced

4.1.2 Approves risk exceptions where patches cannot be applied and reviews related mitigation strategies

4.1.3 Reviews patch status reports and ensures resources are available to meet patching obligations

4.2 IT Support / Internal IT Administrator

4.2.1 Monitors systems for vulnerabilities and available patches using vendor alerts, threat intelligence advisories, and operating system notifications

4.2.2 Applies operating system, firmware, and application updates within defined timeframes

4.2.3 Maintains a formal patch log and documents unresolved or deferred updates

4.2.4 Conducts testing and schedules critical updates to minimize operational disruption

[... 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

9.1.1 This policy must be reviewed at least annually by the General Manager, with input from the IT Provider and Privacy Coordinator

9.2 Review Triggers

9.2.1 Interim reviews must be conducted if:

9.2.1.1 A major vulnerability or exploit affects systems within scope

9.2.1.2 Significant system or software changes occur

9.2.1.3 An audit identifies gaps in patching processes

9.2.1.4 A patching-related incident or breach is recorded

9.3 Policy Version Control

9.3.1 All updates must be recorded in a version log with a summary of changes

9.3.2 Changes must be communicated to affected personnel

9.3.3 Outdated versions must be archived with restricted access

10. Related Policies and Linkages

10.1 This policy supports and depends on several other SME policies:

10.1.1 P12S – Asset Management Policy: Identifies system ownership and classification, ensuring that all assets requiring patching are accounted for and inventoried

10.1.2 P14S – Data Retention Policy and Secure Disposal Policy: Ensures that systems scheduled for decommissioning are securely updated or wiped, reducing vulnerability exposure

10.1.3 P17S – Data Protection and Privacy Policy: Prioritizes vulnerability remediation for systems processing personal data to comply with privacy laws

10.1.4 P22S – Logging and Monitoring Policy: Supports detection of unpatched systems or suspicious behavior that may indicate exploitation of a vulnerability

10.1.5 P30S – Incident Response Policy: Defines procedures for responding to vulnerabilities that result in security incidents, including escalation and reporting steps

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

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

11.2 ISO/IEC 27002

11.2.1 Control 8.8 – Specifies processes for identifying and remediating known technical vulnerabilities in systems

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

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Requires the identification of vulnerabilities and remediation within defined timeframes

11.3.2 SI-2 – Requires prompt application of patches and updates based on severity

11.3.3 CM-2 – Governs system baseline configurations and update documentation to ensure consistent protection

11.4 EU GDPR

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

11.5 EU NIS2 Directive

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

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

11.6 EU DORA

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

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

11.7 COBIT 2019

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

11.7.2 APO12.01 – Aligns risk management with proactive monitoring, threat detection, and correction of system weaknesses