					Insert Registered Legal Entity Name Here							
Document number: P19					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	Systematic treatment of technical vulnerabilities; ongoing effectiveness of security controls.
ISO/IEC 27002:2022	Controls 8.8, 8.9, 5	Implementation guidance for patch management, vulnerability scanning, software integrity, secure configuration, and asset inventory.
NIST SP 800-53 Rev. 5	RA-5, SI-2, CM-2, CM-6	Frequent scanning, flaw remediation, and configuration management are required.
EU GDPR	Article 32, Recital 49	Technical measures for timely patching, vulnerability management, and security continuity.
EU NIS2	Article 21(2)(d)	Detection, response, and mitigation of vulnerabilities to maintain a high level of cyber hygiene.
EU DORA	Articles 8, 10(2)(f)	Timely remediation of ICT vulnerabilities; continuous threat-led assessments.
COBIT 2019	DSS05.02, DSS01.03, MEA	Scan, track, and mitigate technical weaknesses; monitor for exploitation; audit control effectiveness, including patch status.

1. Purpose

1.1 This policy defines the organization's mandatory requirements for identifying, classifying, remediating, and monitoring technical vulnerabilities and software flaws across all information systems and assets within the scope of the Information Security Management System (ISMS).

1.2 It ensures that all known vulnerabilities are assessed and addressed in a risk-based and timely manner through coordinated patching, configuration changes, or compensating controls, in alignment with business needs and compliance obligations.

1.3 This policy supports compliance with ISO/IEC 27001 Annex A Control 8.8 and ISO/IEC 27002 guidance and addresses regulatory requirements under DORA Article 8, NIS2 Article 21, GDPR Article 32, and COBIT 2019 DSS and APO domains.

2. Scope

2.1 This policy applies to all information systems, assets, and environments that store, process, or transmit data subject to ISMS governance, including:

2.1.1 Operating systems, applications, network devices, firmware, cloud platforms, Application Programming Interfaces (APIs), and third-party software.

2.1.2 Systems in development, staging, production, backup, and disaster recovery environments.

2.1.3 Endpoints, servers, Internet of Things (IoT) devices, virtualization infrastructure, and containers.

2.2 It is binding on:

2.2.1 Internal staff: IT administrators, system engineers, application developers, security analysts, and infrastructure teams.

2.2.2 External parties: contractors, managed service providers (MSPs), software vendors, and system integrators with technical responsibilities for in-scope assets.

2.3 This policy covers the full vulnerability and patch management lifecycle, including:

2.3.1 Scanning and detection

2.3.2 Risk classification and prioritization

2.3.3 Patch acquisition, testing, deployment, and rollback

2.3.4 Exception handling and compensating control planning

2.3.5 Logging, reporting, and audit traceability

3. Objectives

3.1 Ensure that all known vulnerabilities are identified, assessed, and remediated in a manner that minimizes risk exposure and aligns with operational priorities.

3.2 Establish consistent, enterprise-wide processes for vulnerability scanning, severity classification (e.g., CVSS), and patch management, including emergency handling and rollback planning.

3.3 Enable secure configuration management through alignment with hardening baselines, change management practices, and real-time threat intelligence.

3.4 Provide measurable compliance with regulatory and standards-based controls related to system integrity, patch hygiene, and timely flaw remediation.

3.5 Define responsibility and accountability across roles for the full vulnerability management lifecycle, ensuring that all stakeholders operate within defined SLAs and reportable control metrics.

3.6 Strengthen audit readiness and improve resilience against emerging threats, including zero-day vulnerabilities, active exploit chains, and significant vendor disclosures.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures its integration into the ISMS.

4.1.2 Defines the enterprise risk posture and ensures alignment with regulatory and control requirements.

4.2 Vulnerability Management Lead / Security Operations Manager

4.2.1 Oversees end-to-end vulnerability and patch management operations.

4.2.2 Coordinates scanning schedules, prioritization models, and remediation timelines.

4.2.3 Maintains the Vulnerability Register and supports the evaluation of compensating controls.

[... 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 This policy shall be reviewed at least annually or upon:

9.1.1 Significant regulatory updates (e.g., changes to DORA, NIS2)

9.1.2 Changes to vulnerability prioritization frameworks (e.g., CVSS updates)

9.1.3 Major changes to the IT environment (e.g., cloud migration, EDR overhaul)

9.1.4 Significant breaches or external advisories requiring policy enhancement

9.2 Reviews shall be conducted by the CISO in collaboration with Security Operations, Risk Management, and Infrastructure Leadership.

9.3 Policy updates must be:

9.3.1 Documented in the ISMS Document Control Register

9.3.2 Reviewed and approved by Top Management

9.3.3 Communicated to all affected stakeholders, including third-party processors

9.4 Historical versions shall be retained securely for audit and accountability purposes.

10. Related Policies and Linkages

10.1 P1 - Information Security Policy. Establishes the overarching commitment to protecting systems and data, including the proactive management of vulnerabilities and assurance of software integrity.

10.2 P5 - Change Management Policy. Governs all patch deployments and configuration changes, requiring documentation, testing, approval, and rollback procedures that support vulnerability remediation processes.

10.3 P6 - Risk Management Policy. Supports the classification and treatment of unremediated vulnerabilities through structured risk assessments, impact analysis, and residual risk acceptance procedures.

10.4 P12 - Asset Management Policy. Ensures systems are inventoried and classified accurately, enabling consistent vulnerability scanning, ownership assignment, and lifecycle patch coverage.

10.5 P22 - Logging and Monitoring Policy. Defines requirements for event detection and audit trail generation. This policy supports visibility into patching activity, unauthorized changes, and exploit attempts targeting known vulnerabilities.

10.6 P30 - Incident Response Policy. Specifies escalation protocols and containment strategies for exploited vulnerabilities, breach investigations, and corrective actions aligned with this policy's controls.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001: Clause 8.1 - Operational Planning and Control: Requires systematic treatment of technical vulnerabilities to ensure the ongoing effectiveness of security controls.

11.2 ISO/IEC 27002:2022 - Controls 8.8, 8.9, 5: Provides implementation guidance for patch management, vulnerability scanning, software integrity, and integration with secure configuration and asset inventory.

11.3 NIST SP 800-53 Rev. 5: RA-5 - Vulnerability Monitoring and Scanning: Requires frequent scanning and remediation tracking. SI-2 - Flaw Remediation: Requires prompt evaluation and mitigation of flaws through available patches or other actions. CM-2 / CM-6 - Configuration Management Baselines and Controls: Establishes the foundation for secure system configurations tied to patch enforcement.

11.4 EU GDPR (2016/679): Article 32 - Security of Processing: Requires implementation of appropriate technical measures, such as timely patching and vulnerability management, to ensure confidentiality and system resilience. Recital 49: Encourages entities to implement preventive controls against known threats to support security and continuity.

11.5 EU NIS2 Directive (2022/2555): Article 21(2)(d): Requires essential and important entities to detect, respond to, and mitigate system vulnerabilities and maintain a high level of cyber hygiene.

11.6 EU DORA (2022/2554): Article 8 - ICT Risk Management: Requires identification and timely remediation of vulnerabilities in information and communication technologies used in financial systems. Article 10(2)(f): Emphasizes continuous threat-led vulnerability assessments and patching as part of operational resilience.

11.7 COBIT 2019: DSS05.02 - Manage Security Vulnerabilities: Directs organizations to scan, track, and mitigate known technical weaknesses. DSS01.03 - Monitor Infrastructure: Ensures systems are monitored for signs of exploitation or weakness. MEA03 - Monitor, Evaluate, and Assess Compliance: Requires regular auditing of control effectiveness, including patch status and exception handling.