<table>
<tr><td colspan="5"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P19</td><td colspan="8">Document Title:
Vulnerability and Patch Management Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="8">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	Controls 8.8, 8.9, 5.23	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	
EU GDPR	Article 32, Recital 49	
EU NIS2	Article 21(2)(d)	
EU DORA	Articles 8, 10(2)(f)	
COBIT 2019	DSS05.02, DSS01.03, MEA03	

PREVIEW ONLY

Legal Notice (Copyright & Usage Restrictions)

© 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.

Unauthorized use is strictly prohibited and may lead to legal action.

For licensing, contact: info@clarysec.com

		[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

1. Purpose

1.1 This policy defines the organization’s mandatory requirements for identifying, classifying, remediating, and monitoring technical vulnerabilities and software flaws in 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 adjustments, 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, APIs, and third-party software.

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

2.1.3 Endpoints, servers, 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 over in-scope assets.

2.3 The policy encompasses the complete vulnerability and patch 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, evaluated, 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 control practices, and real-time threat intelligence.

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

PREVIEW ONLY

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

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

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns the policy and ensures its integration within the ISMS.

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

[….]

11. Reference Standards and Frameworks

This policy aligns with globally accepted standards and regulatory frameworks that define secure system maintenance, flaw remediation, and technical vulnerability management.

ISO/IEC 27001:2022

Clause 8.1 - Operational Planning and Control: Requires systematic treatment of technical vulnerabilities to ensure ongoing effectiveness of security controls.

ISO/IEC 27002:2022 - Controls 8.8, 8.9, 5.23

Provides implementation guidance for patching, vulnerability scanning, software integrity, and integration with secure configuration and asset inventories.

NIST SP 800-53 Rev.5

RA-5 - Vulnerability Monitoring and Scanning: Mandates frequent scanning and remediation tracking.

SI-2 - Flaw Remediation: Requires prompt evaluation and mitigation of flaws with 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.

EU GDPR (2016/679)

Article 32 - Security of Processing: Requires implementation of appropriate technical measures, such as prompt patching and vulnerability treatment, to ensure confidentiality and system resilience.

Recital 49: Encourages entities to implement preventive controls against known threats to support security and continuity.

EU NIS2 Directive (2022/2555)

PREVIEW ONLY

Article 21(2)(d): Obligates essential and important entities to detect, respond to, and mitigate system vulnerabilities and maintain a high level of cyber hygiene.

EU DORA (2022/2554)

Article 8 - ICT Risk Management: Requires identification and timely remediation of vulnerabilities in information and communications technologies used in financial systems.

Article 10(2)(f): Emphasizes continuous threat-led vulnerability assessments and patching as part of operational resilience.

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.

PREVIEW ONLY