					Insert Registered Legal Entity Name Here							
Document number: P39					Document Title: **Coordinated Vulnerability Disclosure 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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
EU GDPR	Art. 32(1)(d)	
EU NIS2	Art. 21(2)(e)	
EU DORA	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Purpose

1.1 Establish a formal process for receiving, handling, and disclosing information about vulnerabilities affecting the organization's systems or services, as required by NIS2 Article 21(2)(e) on vulnerability handling and disclosure.

1.2 Encourage external security researchers, partners, and users to report vulnerabilities responsibly through Coordinated Vulnerability Disclosure (CVD), and define how the organization communicates vulnerability information to stakeholders.

2. Scope

2.1 This policy applies to all network and information systems owned or operated by the organization and to any identified vulnerabilities in those systems.

2.2 It applies to internal teams, including security, IT, and development, as well as any external parties reporting vulnerabilities, such as researchers, customers, and suppliers. It also governs communications with product vendors or service providers where their components are implicated in the vulnerability.

3. Objectives

3.1 Detect and remediate security vulnerabilities in a timely manner by leveraging both internal assessments and external disclosures.

3.2 Provide clear guidance for external reporters to submit vulnerability information safely and lawfully, and for the organization to respond and remediate effectively.

3.3 Ensure alignment with NIS2 requirements and industry best practice, including ISO/IEC 29147 and ISO/IEC 30111, for coordinated vulnerability disclosure, thereby improving overall ecosystem security.

4. Roles and Responsibilities

4.1 Vulnerability Response Team (VRT): A designated team, led by the CISO or Vulnerability Management Lead, responsible for receiving and triaging vulnerability reports, assessing risk and impact, and coordinating remediation and public disclosure.

4.2 IT and Development Teams: Work with the VRT to validate reported vulnerabilities, develop and test patches or mitigation measures, and deploy fixes. Provide technical details for security advisories where required.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Monitoring and Audit

9.1 The VRT shall maintain a vulnerability disclosure log tracking each report from receipt through closure. The log shall be reviewed monthly to ensure timely progression of open items. Overdue items shall be escalated.

9.2 The Internal Audit and Compliance Function, or an independent security assessor, shall annually review the effectiveness of the vulnerability handling process, including verification that sampled vulnerability cases were handled in accordance with this policy, acknowledged, remediated, and disclosed in a timely manner. They shall also verify that the public-facing disclosure channel is operational, including by confirming that test emails are received and acted upon.

9.3 Vulnerability metrics, including volume by severity and remediation times, shall be compiled quarterly and presented to the cybersecurity governance committee to support updates to the Risk Register and risk assessments.

10. Review and Maintenance

10.1 This policy shall be reviewed at least annually. In addition, any significant change in the IT infrastructure, such as the launch of a new internet-facing service, or any relevant regulatory development, such as new EU legal requirements relating to product vulnerability disclosure, shall trigger an out-of-cycle review.

10.2 Updates to this policy shall incorporate feedback from external reporters and lessons learned from internal post-incident analyses. Major changes shall be approved by the CISO, communicated to all employees, and published in the online policy repository for transparency.

11. Related Policies and Linkages

11.1 P01 – Information Security Policy. Management mandate for vulnerability handling and disclosure.

11.2 P19 – Vulnerability and Patch Management Policy. Internal remediation pipeline linked to CVD intake.

11.3 P24 – Secure Development Policy. Supports fixes and Secure Development Lifecycle (SDLC) hardening arising from reported issues.

11.4 P25 – Application Security Requirements Policy. Ensures products include disclosure-ready security requirements.

11.5 P30 – Incident Response Policy. Addresses active exploitation of disclosed vulnerabilities.

11.6 P31 – Evidence Collection and Forensics Policy. Preserves forensic artifacts from reported or exploited flaws.

11.7 P26 – Third-Party and Supplier Security Policy. Coordinates disclosures involving supplier components.

11.8 P37 – Legal and Regulatory Compliance Policy. Governs notifications, safe harbor wording, and publication.

12. References

12.1 NIS2 Directive (EU 2022/2555), Article 21(2), point (e) (security in development and vulnerability handling and disclosure)

12.2 Commission Implementing Regulation (EU) 2024/2690, Annex, Section 6.10 (technical requirements on vulnerability handling and disclosure processes)

12.3 ENISA Technical Guidance on Cybersecurity Risk Management Measures – section on Vulnerability Handling and Disclosure

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (control A.5.7 on threat intelligence and vulnerability disclosure; control A.8.28 on secure development)

12.5 ISO/IEC 29147:2018 (Guidelines for vulnerability disclosure) and ISO/IEC 30111:2019 (Guidelines for vulnerability handling processes)