				[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 where applicable		
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	

Note: P39 Coordinated Vulnerability Disclosure Policy is added to cover the vulnerability disclosure aspect of NIS2 Article 21(2)(e), which the ENT policies only partially addressed. The base ENT policies had internal vulnerability management (patching, scanning) but no mechanism for external parties to report vulnerabilities or for coordinated disclosure – a clear gap, since NIS2 requires handling and disclosure of vulnerabilities. The Implementing Regulation (EU 2024/2690) Section 6.10 specifically calls for establishing vulnerability handling and disclosure processes, and ENISA's guidance highlights the need for CVD policies and a single point of contact. P39 creates a formal CVD program, including safe harbor for researchers and timelines for acknowledgement and remediation, which aligns with international best practices (ISO 29147) and NIS2 expectations. This add-on will enable the organization to demonstrably comply with NIS2's requirement to address vulnerabilities "including disclosure" by having a published policy and process for dealing with reports, thereby filling the previous gap in the matrix. It also ties into Article 7 of the NIS2 Directive (not explicitly asked in Article 21 but relevant) which encourages coordinated vulnerability disclosure at the Member State level.

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 (Coordinated Vulnerability Disclosure - CVD) responsibly, 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 any identified vulnerabilities in those systems.

2.2 It covers internal teams (security, IT, development) and any external parties reporting vulnerabilities (e.g., researchers, customers, suppliers). It also governs communications with product vendors or service providers if their components are involved in the vulnerability.

3. **Objectives**

3.1 Detect and resolve 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 legally, and for the organization to respond and remediate effectively.

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

4. **Roles and Responsibilities**

4.1 Vulnerability Response Team (VRT): A designated team (led by the CISO or Vulnerability Manager) that receives and triages vulnerability reports, assesses risk/impact, and coordinates remediation and public disclosure.

4.2 IT and Development Teams: Work with the VRT to validate reported vulnerabilities, develop and test patches or mitigations, and deploy fixes. Provide technical details for advisories if needed.

4.3 Communications/PR: Prepares and disseminates public vulnerability advisories or notifications to customers, in coordination with VRT, once a fix or mitigation is available or as needed.

4.4 External Reporter (Researcher/Partner/User): Expected to follow the responsible disclosure guidelines defined by this policy when reporting vulnerabilities. In return, the organization will acknowledge and, if applicable, may provide thanks or rewards as outlined.

[……

…….

…….

…….

…….

]

10. **Review and Maintenance**

10.1 This policy will be reviewed at least annually. Additionally, any significant change in our IT environment (e.g., launching a new internet-facing service) or relevant regulatory developments (e.g., new EU laws on product vulnerability disclosure) will trigger an out-of-cycle review.

10.2 Updates to the policy will incorporate feedback from external reporters and lessons from internal post-incident analyses. Major changes will be approved by the CISO and communicated to all employees and published in our security policy repository online 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. Feeds fixes and SDLC hardening from reported issues.

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

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

11.6 P31 – Evidence Collection and Forensics Policy. Preserves artifacts from reported/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 notification, 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 & 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)