					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P39					Titlul documentului: **Politica privind divulgarea coordonată a vulnerabilităților**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
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	
GDPR al UE	Art. 32(1)(d)	
Directiva NIS2 a UE	Art. 21(2)(e)	
Regulamentul DORA al UE	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Scop

1.1 Se stabilește un proces formal pentru primirea, tratarea și divulgarea informațiilor privind vulnerabilitățile care afectează sistemele sau serviciile organizației, în conformitate cu articolul 21 alineatul (2) litera (e) din Directiva NIS2 a UE privind tratarea și divulgarea vulnerabilităților.

1.2 Se încurajează cercetătorii externi în domeniul securității, partenerii și utilizatorii să raporteze vulnerabilitățile în mod responsabil, în cadrul procesului de divulgare coordonată a vulnerabilităților (Coordinated Vulnerability Disclosure - CVD), și se definește modul în care organizația comunică informațiile privind vulnerabilitățile către părțile interesate.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor sistemelor de rețea și informatice deținute sau operate de organizație, precum și tuturor vulnerabilităților identificate în aceste sisteme.

2.2 Aceasta se aplică echipelor interne (securitate, IT, dezvoltare) și oricăror părți externe care raportează vulnerabilități (de exemplu, cercetători, clienți, furnizori). De asemenea, reglementează comunicările cu furnizorii de produse sau prestatorii de servicii, dacă componentele acestora sunt implicate în vulnerabilitate.

3. Obiective

3.1 Detectarea și remedierea în timp util a vulnerabilităților de securitate, prin utilizarea atât a evaluărilor interne, cât și a divulgărilor externe.

3.2 Furnizarea unor instrucțiuni clare pentru raportorii externi, astfel încât aceștia să transmită informațiile privind vulnerabilitățile în condiții de siguranță și în mod legal, iar organizația să poată răspunde și remedia în mod eficace.

3.3 Asigurarea alinierii la cerințele NIS2 și la bunele practici din industrie (ISO/IEC 29147 și ISO/IEC 30111) pentru divulgarea coordonată a vulnerabilităților, în vederea îmbunătățirii securității generale a ecosistemului.

4. Roluri și responsabilități

4.1 Echipa de răspuns la vulnerabilități (VRT): echipă desemnată, condusă de Directorul pentru securitatea informațiilor sau de Responsabilul cu managementul vulnerabilităților, care primește și triază rapoartele de vulnerabilitate, evaluează riscul/impactul și coordonează remedierea și divulgarea publică.

4.2 Echipele IT și de dezvoltare: colaborează cu VRT pentru a valida vulnerabilitățile raportate, a dezvolta și testa patch-uri sau măsuri de atenuare și a implementa remedierile. Acestea furnizează, dacă este necesar, detalii tehnice pentru informări.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Monitorizare și audit

9.1 VRT va menține un registru al divulgării vulnerabilităților, care urmărește fiecare raport de la primire până la închidere. Acest registru va fi revizuit lunar pentru a asigura progresul la timp al elementelor deschise. Elementele restante vor fi escaladate.

9.2 Auditul Intern sau un evaluator independent de securitate va revizui anual eficacitatea procesului de tratare a vulnerabilităților, de exemplu verificând dacă eșantioane de cazuri de vulnerabilitate au fost gestionate conform politicii (confirmate, remediate și divulgate în timp util). De asemenea, va verifica dacă canalul public de divulgare destinat sistemelor expuse public este funcțional (de exemplu, dacă e-mailurile de test sunt primite și tratate corespunzător).

9.3 Indicatorii privind vulnerabilitățile (volum în funcție de severitate, timpi de remediere etc.) vor fi compilați trimestrial și prezentați comitetului de guvernanță în domeniul securității cibernetice, pentru a fundamenta actualizările evaluării riscurilor.

10. Revizuire și mentenanță

10.1 Această politică va fi revizuită cel puțin anual. În plus, orice schimbare semnificativă în mediul nostru IT (de exemplu, lansarea unui nou serviciu expus la internet) sau orice evoluție relevantă în materie de reglementare (de exemplu, noi acte normative ale UE privind divulgarea vulnerabilităților produselor) va declanșa o revizuire în afara ciclului obișnuit.

10.2 Actualizările politicii vor integra feedbackul raportorilor externi și lecțiile rezultate din analizele interne post-incident. Schimbările majore vor fi aprobate de Directorul pentru securitatea informațiilor, comunicate tuturor angajaților și publicate în depozitul central online de politici, pentru transparență.

11. Politici conexe și interdependențe

11.1 P01 – Politica de securitate a informației. Stabilește mandatul managementului pentru tratarea și divulgarea vulnerabilităților.

11.2 P19 – Politica de management al vulnerabilităților și patch-urilor. Definește fluxul intern de remediere asociat preluării raportărilor CVD.

11.3 P24 – Politica de dezvoltare securizată. Integrează remedierile și consolidarea SDLC pe baza problemelor raportate.

11.4 P25 – Politica privind cerințele de securitate a aplicațiilor. Asigură că produsele au cerințe de securitate adecvate pentru divulgare.

11.5 P30 – Politica de răspuns la incidente. Reglementează exploatarea activă a vulnerabilităților divulgate.

11.6 P31 – Politica privind colectarea dovezilor și activitățile criminalistice. Asigură păstrarea artefactelor rezultate din deficiențe raportate sau exploatate.

11.7 P26 – Politica de securitate privind terții și furnizorii. Coordonează divulgările care implică componente ale furnizorilor.

11.8 P37 – Politica privind conformitatea juridică și de reglementare. Reglementează notificarea, formulările privind clauza de protecție și publicarea.

12. Referințe

12.1 Directiva NIS2 (UE 2022/2555), articolul 21 alineatul (2), litera (e) (securitatea în dezvoltare și tratarea și divulgarea vulnerabilităților)

12.2 Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei, anexa, secțiunea 6.10 (cerințe tehnice privind procesele de tratare și divulgare a vulnerabilităților)

12.3 Ghidul tehnic ENISA privind măsurile de management al riscurilor de securitate cibernetică – secțiunea privind tratarea și divulgarea vulnerabilităților

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (controlul A.5.7 privind informațiile despre amenințări și divulgarea vulnerabilităților; controlul A.8.28 privind dezvoltarea securizată)

12.5 ISO/IEC 29147:2018 (linii directoare pentru divulgarea vulnerabilităților) și ISO/IEC 30111:2019 (linii directoare pentru procesele de tratare a vulnerabilităților)