					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P19					Titlul documentului: **Politica de management al vulnerabilităților și al patch-urilor**							
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	Clauza 8	Tratarea sistematică a vulnerabilităților tehnice; eficacitatea continuă a controalelor de securitate.
ISO/IEC 27002:2022	Controalele 8.8, 8.9, 5	Ghid de implementare pentru aplicarea patch-urilor, scanarea vulnerabilităților, integritatea software-ului, configurarea securizată și inventarierea activelor.
NIST SP 800-53 Rev. 5	RA-5, SI-2, CM-2, CM-6	Impune scanări frecvente, remedierea defectelor și managementul configurației.
GDPR	Articolul 32, Considerentul 49	Măsuri tehnice pentru aplicarea promptă a patch-urilor, tratarea vulnerabilităților și menținerea securității.
Directiva NIS2	Articolul 21(2)(d)	Detectarea, răspunsul și atenuarea vulnerabilităților pentru menținerea unui nivel ridicat de igienă cibernetică.
Regulamentul DORA	Articolele 8, 10(2)(f)	Remedierea la timp a vulnerabilităților TIC; evaluări continue orientate de amenințări.
COBIT 2019	DSS05.02, DSS01.03, MEA	Scanarea, urmărirea și atenuarea punctelor slabe tehnice; monitorizarea pentru identificarea exploatării; auditarea eficacității, inclusiv a stării patch-urilor.

1. Scop

1.1 Această politică stabilește cerințele obligatorii ale organizației pentru identificarea, clasificarea, remedierea și monitorizarea vulnerabilităților tehnice și a defectelor software din toate sistemele informatice și activele aflate în domeniul de aplicare al Sistemului de Management al Securității Informației (SMSI).

1.2 Aceasta asigură că toate vulnerabilitățile cunoscute sunt evaluate și tratate în timp util, pe baza riscului, prin aplicarea coordonată a patch-urilor, ajustări de configurare sau controale compensatorii, în concordanță cu nevoile organizației și obligațiile de conformitate.

1.3 Această politică sprijină conformitatea cu controlul 8.8 din Anexa A la ISO/IEC 27001 și cu ghidul ISO/IEC 27002 și răspunde cerințelor de reglementare prevăzute la articolul 8 din DORA, articolul 21 din NIS2, articolul 32 din GDPR și domeniile DSS și APO din COBIT 2019.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor sistemelor informatice, activelor și mediilor care stochează, prelucrează sau transmit date aflate sub guvernanța SMSI, inclusiv:

2.1.1 sisteme de operare, aplicații, echipamente de rețea, firmware, platforme cloud, API-uri și software terț.

2.1.2 sisteme din mediile de dezvoltare, testare, producție, backup și recuperare în caz de dezastru.

2.1.3 stații de lucru, servere, dispozitive din Internetul obiectelor (IoT), infrastructură de virtualizare și containere.

2.2 Este obligatorie pentru:

2.2.1 personalul intern: administratori IT, ingineri de sistem, dezvoltatori de aplicații, analiști de securitate și echipe de infrastructură.

2.2.2 părțile externe: contractori, furnizori de servicii administrate (MSP), furnizori de software și integratori de sisteme cu responsabilități tehnice asupra activelor incluse în domeniul de aplicare.

2.3 Politica acoperă întregul ciclu de viață al managementului vulnerabilităților și al patch-urilor, inclusiv:

2.3.1 scanarea și detectarea

2.3.2 clasificarea și prioritizarea riscurilor

2.3.3 obținerea, testarea, implementarea și revenirea patch-urilor

2.3.4 gestionarea excepțiilor și planificarea controalelor compensatorii

2.3.5 jurnalizarea, raportarea și trasabilitatea în scop de audit

3. Obiective

3.1 Să asigure că toate vulnerabilitățile cunoscute sunt identificate, evaluate și remediate într-un mod care reduce la minimum expunerea la risc și se aliniază priorităților operaționale.

3.2 Să stabilească procese consecvente, la nivelul întregii organizații, pentru scanarea vulnerabilităților, clasificarea severității (de exemplu, CVSS) și managementul patch-urilor, inclusiv tratarea situațiilor de urgență și planificarea revenirii.

3.3 Să permită managementul configurației securizate prin alinierea la configurațiile de referință pentru hardening, practicile de control al schimbărilor și informațiile privind amenințările în timp real.

3.4 Să asigure conformitate măsurabilă cu controalele prevăzute de reglementări și standarde privind integritatea sistemelor, igiena patch-urilor și remedierea la timp a defectelor.

3.5 Să definească responsabilitatea și răspunderea pe roluri pentru întregul ciclu de viață al managementului vulnerabilităților, asigurând că toate părțile interesate acționează în limitele SLA-urilor definite și ale indicatorilor de control raportați.

3.6 Să consolideze pregătirea pentru audit și să îmbunătățească reziliența în fața riscurilor emergente, inclusiv vulnerabilități de tip zero-day, lanțuri active de exploatare și notificări critice din partea furnizorilor.

4. Roluri și responsabilități

4.1 Directorul pentru securitatea informațiilor (CISO)

4.1.1 Deține această politică și asigură integrarea acesteia în cadrul SMSI.

4.1.2 Definește profilul de risc al organizației și asigură alinierea la cerințele de reglementare și de control.

4.2 Responsabilul pentru managementul vulnerabilităților / Managerul operațiunilor de securitate

4.2.1 Asigură supravegherea integrală a operațiunilor de management al vulnerabilităților și al patch-urilor.

4.2.2 Coordonează planificarea scanărilor, modelele de prioritizare și termenele de remediere.

4.2.3 Menține Registrul vulnerabilităților și colaborează la evaluarea controalelor compensatorii.

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

9. Cerințe de revizuire și actualizare

9.1 Această politică trebuie revizuită cel puțin anual sau la apariția oricăreia dintre următoarele situații:

9.1.1 actualizări semnificative ale cerințelor de reglementare (de exemplu, modificări ale DORA, NIS2)

9.1.2 modificări ale cadrelor de prioritizare a vulnerabilităților (de exemplu, actualizări CVSS)

9.1.3 schimbări majore ale mediului IT (de exemplu, migrare către cloud, modernizare majoră a EDR)

9.1.4 incidente majore de securitate sau notificări externe care impun consolidarea politicii

9.2 Revizuirile trebuie efectuate de CISO în colaborare cu operațiunile de securitate, managementul riscurilor și conducerea infrastructurii.

9.3 Actualizările politicii trebuie:

9.3.1 să fie documentate în registrul de control al documentelor al SMSI

9.3.2 să fie revizuite și aprobate de conducerea executivă

9.3.3 să fie comunicate tuturor părților interesate afectate, inclusiv terților împuterniciți

9.4 Versiunile istorice trebuie păstrate în condiții de securitate în scopuri de audit și trasabilitate.

10. Politici asociate și interdependențe

10.1 P1 - Politica de securitate a informației. Stabilește angajamentul general de protejare a sistemelor și datelor, inclusiv managementul proactiv al vulnerabilităților și asigurarea integrității software-ului.

10.2 P5 - Politica de management al schimbărilor. Guvernează implementarea tuturor patch-urilor și ajustărilor de configurare, impunând documentare, testare, aprobare și proceduri de revenire care completează procesele de remediere a vulnerabilităților.

10.3 P6 - Politica de management al riscurilor. Sprijină clasificarea și tratarea vulnerabilităților neremediate prin evaluări structurate ale riscurilor, analiza impactului și proceduri de acceptare a riscului rezidual.

10.4 P12 - Politica de management al activelor. Asigură inventarierea și clasificarea corectă a sistemelor, permițând scanări consecvente de vulnerabilitate, atribuirea responsabilității și acoperirea cu patch-uri pe întregul ciclu de viață.

10.5 P22 - Politica de jurnalizare și monitorizare. Definește cerințele pentru detectarea evenimentelor și generarea pistei de audit. Această politică susține vizibilitatea asupra activităților de aplicare a patch-urilor, modificărilor neautorizate și tentativelor de exploatare care vizează vulnerabilități cunoscute.

10.6 P30 - Politica de răspuns la incidente. Specifică protocoalele de escaladare și strategiile de conținere pentru vulnerabilități exploatate, investigații privind incidente de securitate și acțiuni corective aliniate controalelor prevăzute de această politică.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001: Clauza 8.1 - Planificare și control operațional: impune tratarea sistematică a vulnerabilităților tehnice pentru a asigura eficacitatea continuă a controalelor de securitate.

11.2 ISO/IEC 27002:2022 - Controalele 8.8, 8.9, 5: oferă îndrumări de implementare pentru aplicarea patch-urilor, scanarea vulnerabilităților, integritatea software-ului și integrarea cu configurarea securizată și inventarierea activelor.

11.3 NIST SP 800-53 Rev. 5: RA-5 - monitorizarea și scanarea vulnerabilităților: impune scanări frecvente și urmărirea remedierii. SI-2 - remedierea defectelor: impune evaluarea și atenuarea promptă

a defectelor pentru care există patch-uri sau alte măsuri disponibile. CM-2 / CM-6 - baze de referință și controale pentru managementul configurației: stabilește fundamentul pentru configurații securizate ale sistemelor, corelate cu aplicarea patch-urilor.

11.4 GDPR (UE) 2016/679: Articolul 32 - Securitatea prelucrării: impune implementarea unor măsuri tehnice adecvate, precum aplicarea promptă a patch-urilor și tratarea vulnerabilităților, pentru a asigura confidențialitatea și reziliența sistemelor. Considerentul 49: încurajează entitățile să implementeze controale preventive împotriva amenințărilor cunoscute pentru a susține securitatea și continuitatea.

11.5 Directiva NIS2 (UE) 2022/2555: Articolul 21(2)(d): obligă entitățile esențiale și importante să detecteze, să răspundă la și să atenueze vulnerabilitățile sistemelor și să mențină un nivel ridicat de igienă cibernetică.

11.6 Regulamentul DORA (UE) 2022/2554: Articolul 8 - Managementul riscurilor TIC: impune identificarea și remedierea la timp a vulnerabilităților din tehnologiile informației și comunicațiilor utilizate în sistemele financiare. Articolul 10(2)(f): subliniază evaluările continue ale vulnerabilităților orientate de amenințări și aplicarea patch-urilor ca parte a rezilienței operaționale.

11.7 COBIT 2019: DSS05.02 - managementul vulnerabilităților de securitate: stabilește că organizațiile trebuie să scaneze, să urmărească și să atenueze punctele slabe tehnice cunoscute. DSS01.03 - monitorizarea infrastructurii: asigură monitorizarea sistemelor pentru identificarea semnelor de exploatare sau a punctelor slabe. MEA03 - monitorizarea, evaluarea și analiza conformității: impune auditarea periodică a eficacității controalelor, inclusiv a stării patch-urilor și a tratării excepțiilor.