					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P19S					Titlul documentului: **Politica de management al vulnerabilităților și 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**

Aliniere la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	
ISO/IEC 27002:2022	Controalele 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Directiva UE NIS2	Articolele 21(2)(d), 21(2)(e)	
Regulamentul UE DORA	Articolele 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR	Articolul 32(1)(b)	

1. Scop

1.1 Prezenta politică stabilește modul în care organizația identifică, evaluează și remediază vulnerabilitățile la nivelul sistemelor, aplicațiilor și infrastructurii.

1.2 Scopul acesteia este de a reduce riscul de securitate cibernetică prin impunerea aplicării la timp a patch-urilor și a practicilor de remediere bazate pe risc, adecvate întreprinderilor mici și mijlocii (IMM-uri).

1.3 Această politică sprijină conformitatea cu cerințele de certificare ISO/IEC 27001:2022 și contribuie la îndeplinirea obligațiilor de reglementare în temeiul GDPR, NIS2 și DORA, prin impunerea unui management proactiv al vulnerabilităților tehnice.

1.4 Organizația recunoaște că sistemele neactualizate reprezintă o amenințare semnificativă la adresa securității informațiilor și trebuie tratate în mod sistematic și fără întârziere.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor:

2.1.1 tuturor serverelor, stațiilor de lucru, laptopurilor, dispozitivelor mobile, echipamentelor de rețea și platformelor cloud utilizate de organizație;

2.1.2 tuturor sistemelor de operare, aplicațiilor software ale terților, modulelor software și aplicațiilor utilizate în activitățile operaționale ale organizației;

2.1.3 personalului IT intern sau furnizorilor externi de servicii responsabili pentru mentenanța, actualizarea sau monitorizarea sistemelor;

2.1.4 oricărui cod dezvoltat la comandă sau software integrat administrat de organizație ori în numele acesteia.

2.2 Politica acoperă atât infrastructura administrată direct de organizație, cât și sistemele administrate de furnizori contractați sau furnizori de găzduire.

3. Obiective

3.1 Identificarea și evaluarea în timp util și în mod consecvent a vulnerabilităților cunoscute la nivelul tuturor activelor IT.

3.2 Aplicarea patch-urilor și a actualizărilor software în funcție de severitate și de riscul pentru activitățile organizației sau pentru datele cu caracter personal.

3.3 Prevenirea exploatării slăbiciunilor tehnice care ar putea conduce la întreruperea serviciilor, la o încălcare a securității datelor sau la neconformitate legală.

3.4 Menținerea unor evidențe exacte privind patch-urile aplicate, problemele restante și excepțiile, pentru a asigura pregătirea pentru audit.

3.5 Utilizarea unor instrumente și procese adecvate dimensiunii organizației și complexității sale operaționale, fără a compromite eficacitatea.

3.6 Sprijinirea conformității legale și de reglementare, inclusiv cu articolul 32 din GDPR și cu controlul 8 din Anexa A la ISO.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Are responsabilitatea generală de a asigura implementarea activităților de management al vulnerabilităților și patch-urilor.

4.1.2 Aprobă excepțiile de risc atunci când patch-urile nu pot fi aplicate și revizuiește strategiile de atenuare aferente.

4.1.3 Revizuiește rapoartele privind stadiul aplicării patch-urilor și se asigură că sunt disponibile resursele necesare pentru îndeplinirea obligațiilor aferente.

4.2 Furnizor de servicii IT / Administrator IT intern

4.2.1 Monitorizează sistemele pentru identificarea vulnerabilităților și a patch-urilor disponibile, utilizând alerte ale furnizorilor, informări privind amenințările și notificări la nivelul sistemului de operare.

4.2.2 Aplică actualizările sistemului de operare, firmware-ului și aplicațiilor în termenele stabilite.

4.2.3 Menține un registru formal al patch-urilor și documentează actualizările neaplicate sau amânate.

4.2.4 Efectuează testarea și planificarea actualizărilor critice pentru a reduce la minimum perturbările operaționale.

[... 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 Revizuire anuală

9.1.1 Această politică trebuie revizuită cel puțin o dată pe an de Directorul general, cu contribuția Furnizorului IT și a Responsabilului cu protecția datelor.

9.2 Factori declanșatori ai revizuirii

9.2.1 Revizuirile intermediare trebuie efectuate dacă:

9.2.1.1 o vulnerabilitate majoră sau un exploit afectează sistemele incluse în domeniul de aplicare;

9.2.1.2 au loc schimbări semnificative la nivelul sistemelor sau software-ului;

9.2.1.3 un audit identifică lacune în procesele de aplicare a patch-urilor;

9.2.1.4 este înregistrat un incident sau o încălcare asociată aplicării patch-urilor.

9.3 Controlul versiunilor politicii

9.3.1 Toate actualizările trebuie înregistrate într-un jurnal al versiunilor, cu un rezumat al modificărilor.

9.3.2 Modificările trebuie comunicate personalului afectat.

9.3.3 Versiunile depășite trebuie arhivate cu acces restricționat.

10. Politici asociate și interdependențe

10.1 Această politică sprijină și depinde de mai multe alte politici SME:

10.1.1 P12S – Politica de management al activelor: identifică proprietatea și clasificarea sistemelor, asigurând că toate activele care necesită aplicarea patch-urilor sunt evidențiate și inventariate;

10.1.2 P14S – Politica de păstrare și eliminare a datelor: asigură că sistemele programate pentru dezafectare sunt actualizate în condiții de securitate sau șterse, reducând expunerea la vulnerabilități;

10.1.3 P17S – Politica de protecție a datelor și confidențialitate: prioritizează remedierea vulnerabilităților pentru sistemele care prelucrează date cu caracter personal, în vederea respectării legislației privind protecția datelor;

10.1.4 P22S – Politica de jurnalizare și monitorizare: sprijină detectarea sistemelor neactualizate sau a comportamentelor suspecte care pot semnala exploatarea unei vulnerabilități;

10.1.5 P30S – Politica de răspuns la incidente: definește procedurile de răspuns la vulnerabilitățile care conduc la incidente de securitate, inclusiv pașii de escaladare și raportare.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – impune implementarea controalelor pentru tratarea riscurilor operaționale, inclusiv managementul vulnerabilităților.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.8 – specifică procese pentru scanarea și remedierea vulnerabilităților cunoscute la nivelul sistemelor.

11.2.2 Controlul 8.9 – subliniază configurarea securizată, validarea patch-urilor și controlul schimbărilor pentru a evita noi expuneri în timpul actualizărilor.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – impune identificarea vulnerabilităților și remedierea acestora în termene definite.

11.3.2 SI-2 – impune aplicarea promptă a patch-urilor și actualizărilor în funcție de severitate.

11.3.3 CM-2 – reglementează configurațiile de referință ale sistemelor și documentarea actualizărilor pentru a asigura protecții consecvente.

11.4 GDPR

11.4.1 Articolul 32(1)(b) – impune organizațiilor să implementeze măsuri tehnice adecvate, inclusiv aplicarea patch-urilor, pentru a menține securitatea prelucrării.

11.5 Directiva UE NIS2

11.5.1 Articolul 21(2)(d) – impune tratarea vulnerabilităților prin scanare sistematică și remediere.

11.5.2 Articolul 21(2)(e) – obligă la configurare securizată și managementul patch-urilor pentru a asigura reziliența TIC.

11.6 Regulamentul UE DORA

11.6.1 Articolul 8(1) – impune detectarea și atenuarea riscurilor TIC, inclusiv a vulnerabilităților tehnice.

11.6.2 Articolul 10(2) – impune entităților financiare să remedieze slăbiciunile care afectează sistemele și operațiunile TIC.

11.7 COBIT 2019

11.7.1 DSS05.02 – impune tratarea vulnerabilităților tehnice cunoscute pentru menținerea unor operațiuni securizate.

11.7.2 APO12.01 – aliniază managementul riscurilor cu monitorizarea proactivă și remedierea slăbiciunilor sistemelor.