					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P20					Titlul documentului: **Politica privind protecția punctelor terminale / protecția antimalware**							
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	Sunt necesare controale pentru securitatea punctelor terminale și măsuri antimalware pentru îndeplinirea obiectivelor SMSI
ISO/IEC 27002:2022	Controalele 8.7, 8	Oferă controale tehnice și îndrumări privind măsurile antimalware, apărarea punctelor terminale și managementul incidentelor
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definește cerințe privind protecția împotriva codului malițios, monitorizarea centralizată și configurația de referință
GDPR	Articolul 32	Impune măsuri tehnice adecvate pentru protejarea datelor cu caracter personal, inclusiv protecția împotriva malware-ului
Directiva NIS2	Articolul 21(2)(d)	Impune implementarea măsurilor de detectare a amenințărilor la nivelul punctelor terminale și a măsurilor preventive
Regulamentul DORA	Articolul 9	Impune managementul riscurilor TIC pentru malware și apărarea împotriva amenințărilor provenite de la punctele terminale
COBIT 2019	DSS05.01, DSS01.04, MEA	Impune protecția, monitorizarea și evaluarea controalelor pentru punctele terminale

1. Scop

1.1 Această politică definește controalele obligatorii și cerințele operaționale pentru protejarea punctelor terminale ale organizației — inclusiv stații de lucru, laptopuri, dispozitive mobile și servere — împotriva malware-ului și a amenințărilor asociate.

1.2 Aceasta stabilește standardele minime pentru protecția punctelor terminale, detectarea malware-ului, răspunsul de conținere și monitorizarea comportamentală, astfel încât sistemele să rămână reziliente atât împotriva variantelor comune, cât și a celor avansate de malware.

1.3 Politica sprijină direct conformitatea cu ISO/IEC 27001:2022, Clauza 8.1 și Anexa A, Controlul 8.7, și este aliniată cu obligațiile regionale de securitate cibernetică prevăzute de GDPR, NIS2 și DORA.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor punctelor terminale, inclusiv:

2.1.1 stațiilor de lucru, laptopurilor, dispozitivelor mobile și instanțelor virtuale deținute sau administrate de organizație

2.1.2 dispozitivelor personale autorizate în baza Politicii privind utilizarea dispozitivelor personale (sub rezerva instalării MDM sau a unui agent pentru puncte terminale)

2.1.3 serverelor și activelor de infrastructură, inclusiv mașinilor virtuale găzduite în cloud și dispozitivelor edge

2.1.4 sistemelor de operare, driverelor, serviciilor locale, agenților pentru puncte terminale și controalelor de securitate instalate pe fiecare nod

2.2 Această politică se aplică tuturor persoanelor care au responsabilități administrative, tehnice sau operaționale pentru orice punct terminal, inclusiv:

2.2.1 angajaților interni și contractanților

2.2.2 furnizorilor de servicii administrate (MSP), echipelor externalizate de suport pentru stații de lucru și administratorilor IT terți

2.2.3 utilizatorilor autorizați să opereze sisteme portabile, laptopuri cu VPN activ sau acces mobil la rețelele organizației

2.3 Amenințările acoperite de prezenta politică includ, fără a se limita la:

2.3.1 viruși, viermi, troieni, ransomware, spyware, rootkit-uri, adware, keylogger-e, botnet-uri

2.3.2 malware fără fișiere, încărcături zero-day, malware pentru escaladarea privilegiilor și kituri de exploatare a browserului

2.3.3 cod malițios livrat prin medii amovibile, vectori de phishing, descărcări de tip drive-by sau atacuri bazate pe USB

3. Obiective

3.1 Protejarea integrității, disponibilității și confidențialității sistemelor endpoint și a datelor pe care le prelucrează prin prevenirea, detectarea și răspunsul fiabil la malware.

3.2 Prevenirea executării sau propagării codului malițios în rețelele organizației prin aplicarea măsurilor tehnice de protecție, a configurațiilor de hardening de referință și a telemetriei în timp real.

3.3 Integrarea protecției punctelor terminale cu alte controale ale SMSI, inclusiv managementul vulnerabilităților, controlul accesului, jurnalizarea, monitorizarea și răspunsul la incidente.

3.4 Asigurarea vizibilității continue asupra punctelor terminale prin platforme de protecție gestionate centralizat, inclusiv antivirus/agenți antimalware, detectare și răspuns la nivel de punct terminal (EDR) și telemetrie SIEM.

3.5 Respectarea cerințelor legale, de reglementare și bazate pe standarde care impun securitatea punctelor terminale (de exemplu, articolul 32 din GDPR, articolul 21 din NIS2, articolul 9 din DORA).

3.6 Definirea rolurilor responsabile, aplicarea acordurilor privind nivelul serviciilor (SLA) pentru patch-uri și răspuns la alerte și asigurarea capacității de a demonstra conformitatea prin documentare și raportare.

4. Roluri și responsabilități

4.1 Directorul de securitate a informației (CISO)

4.1.1 Deține această politică și asigură alinierea ei la SMSI și la strategia generală de securitate.

4.1.2 Revizuiește trimestrial indicatorii privind protecția punctelor terminale, tendințele incidentelor și eficacitatea instrumentelor.

4.1.3 Aprobă excepțiile și acceptările de risc rezidual legate de acoperirea punctelor terminale.

4.2 Responsabilul cu securitatea punctelor terminale / Managerul SOC

4.2.1 Gestionează sistemele de protecție a punctelor terminale (de exemplu, AV, EDR, MDM).

4.2.2 Asigură supravegherea aplicării politicii, ajustarea mecanismelor de detectare a amenințărilor și a playbook-urilor de răspuns.

4.2.3 Menține statistici privind acoperirea, registre ale incidentelor malware și configurații de referință pentru alerte.

[... 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 anual sau atunci când:

9.1.1 apar campanii majore de malware sau incidente de securitate a punctelor terminale

9.1.2 noi tipuri de amenințări (de exemplu, malware fără fișiere, variante de ransomware) impun actualizarea strategiilor de detectare sau răspuns

9.1.3 platformele de protecție a punctelor terminale sau arhitecturile agenților se modifică semnificativ

9.1.4 sunt actualizate cerințele legale sau de reglementare care afectează controalele pentru punctele terminale

9.2 Revizuirea trebuie inițiată de responsabilul cu securitatea punctelor terminale și coordonată cu funcțiile CISO, juridic, risc și audit.

9.3 Revizuirile aprobate trebuie documentate în registrul de control al documentelor SMSI, trebuie să primească un nou identificator de versiune și trebuie comunicate tuturor părților afectate.

9.4 Versiunile înlocuite trebuie arhivate, cu acces restricționat, și păstrate pentru integritatea pistei de audit, conform termenelor de retenție ale SMSI.

10. Politici asociate și interdependențe

10.1 P1 - Politica de securitate a informației. Stabilește principiile fundamentale pentru protecția sistemelor, datelor și rețelelor. Prezenta politică aplică aceste principii la nivelul punctelor terminale prin controale tehnice și procedurale antimalware.

10.2 P4 - Politica de control al accesului. Definește restricțiile de acces ale utilizatorilor, aplicate și la nivelul punctelor terminale, inclusiv protecții împotriva escaladării privilegiilor și a instalării neautorizate de software neverificat.

10.3 P5 - Politica de management al schimbărilor. Asigură că actualizările software-ului de protecție a punctelor terminale, ale regulilor de politică sau ale configurațiilor agenților sunt supuse aprobării și unor procese controlate de implementare.

10.4 P12 - Politica de management al activelor. Oferă clasificarea activelor și baza de inventariere necesare pentru vizibilitatea punctelor terminale, acoperirea cu patch-uri și definirea domeniului de aplicare al protecției antimalware.

10.5 P22 - Politica de jurnalizare și monitorizare. Permite integrarea alertelor endpoint, a stării de sănătate a agenților și a informațiilor privind amenințările în sisteme SIEM centralizate pentru detectare în timp real și trasabilitate criminalistică.

10.6 P30 - Politica de răspuns la incidente. Corelează incidentele malware de la nivelul punctelor terminale cu fluxuri de lucru standardizate de conținere, eradicare, investigare și recuperare, cu roluri alocate și praguri de escaladare.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:

11.1.1 Clauza 8.1 - Planificare și control operațional: impune implementarea controalelor tehnice, inclusiv a măsurilor de protecție pentru punctele terminale, pentru menținerea obiectivelor SMSI.

11.2 ISO/IEC 27002:2022 - Controalele 8.7, 8:

11.2.1 Oferă îndrumări tehnice detaliate privind măsurile antimalware, implementarea securizată a software-ului, monitorizarea și pregătirea pentru incidente în mediile endpoint.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Protecția împotriva codului malițios: impune utilizarea instrumentelor antimalware cu scanare în timp real, la acces, și analiză comportamentală.

11.3.2 SI-4 - Monitorizarea sistemului: sprijină integrarea telemetriei cu platforme centralizate de detectare.

11.3.3 CM-6 - Setări de configurare: consolidează setările de control de referință pe punctele terminale, inclusiv aplicarea agenților de protecție.

11.4 GDPR (UE) 2016/679:

11.4.1 Articolul 32 - Securitatea prelucrării: impune organizațiilor să implementeze măsuri tehnice adecvate pentru protejarea datelor cu caracter personal, inclusiv protecția împotriva amenințărilor malware.

11.5 Directiva NIS2 (UE) 2022/2555:

11.5.1 Articolul 21(2)(d): obligă entitățile să implementeze măsuri de detectare și prevenire a amenințărilor, inclusiv mecanisme de apărare antimalware la nivel de punct terminal.

11.6 DORA (UE) 2022/2554:

11.6.1 Articolul 9 - Cerințe privind managementul riscurilor TIC: impune entităților financiare să adopte măsuri de protecție pentru prevenirea, detectarea și răspunsul la malware și la amenințările provenite de la punctele terminale.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protecție împotriva malware-ului: impune detectarea și atenuarea malware-ului la nivelul tuturor punctelor terminale ale organizației.

11.7.2 DSS01.04 - Gestionarea disponibilității și capacității: asigură echilibrarea protecției antimalware cu performanța sistemelor și continuitatea activității.

11.7.3 MEA03 - Monitorizare, evaluare și analiză a conformității: impune auditarea periodică a controalelor endpoint și a eficacității protecției.