| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Introduceți aici denumirea entității juridice înregistrate | | | | | | | |
| Numărul documentului:<br>P20S | | | | | Titlul documentului:<br>**Politica privind protecția punctelor terminale împotriva malware-ului** | | | | | | | |
| Versiunea:<br>1.0 | | Data intrării în vigoare:<br>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** |
| | | | |
| | | | |

**Notă juridică (drepturi de autor și restricții de utilizare)**

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

Aliniată la standardele și reglementările aplicabile

| Standard/reglementare | Clauză/articol | Comentariu |
|---|---|---|
| ISO/IEC 27001:2022 | Clauza 8 | Controale operaționale pentru protecția împotriva malware-ului |
| ISO/IEC 27002:2022 | Control 8 | Măsuri de control pentru protecția punctelor terminale |
| NIST SP 800-53 Rev.5 | SI-3, SI-4 | Protecție împotriva codului malițios și răspuns la incidente |
| Directiva NIS2 a UE | Articolele 21(2)(d), (e) | Malware și managementul riscurilor pentru entitățile esențiale și importante |
| Regulamentul DORA al UE | Articolele 10(1), 15 | Reziliență operațională și verificarea terților |
| COBIT 2019 | DSS05.02, DSS05.04 | Protecția punctelor terminale și a rețelei și monitorizare |
| GDPR al UE | Articolele 32(1)(b), 33 | Măsuri tehnice și organizatorice și notificarea încălcărilor |

**1. Scop**

1.1 Această politică definește cerințele minime tehnice, procedurale și comportamentale pentru protejarea tuturor punctelor terminale — inclusiv laptopuri, desktopuri, dispozitive mobile și medii portabile — împotriva codului malițios, inclusiv viruși, ransomware, spyware, rootkit-uri și alte amenințări de tip malware.

1.2 Scopul acesteia este de a asigura că punctele terminale sunt echipate, întreținute și utilizate în moduri care reduc riscul de infectare cu malware, de propagare a acestuia și de compromitere a sistemelor.

1.3 Organizația recunoaște că punctele terminale reprezintă vectori uzuali de intrare pentru malware și, prin urmare, trebuie să fie hardenizate, monitorizate și protejate prin mai multe straturi de apărare.

1.4 Politica sprijină obiectivele organizației privind certificarea ISO/IEC 27001:2022 și este aliniată cu Regulamentul general privind protecția datelor al UE (GDPR), Directiva NIS2, Regulamentul privind reziliența operațională digitală (DORA) și alte cadre relevante.

**2. Domeniu de aplicare**

**2.1 Această politică se aplică:**

2.1.1 Tuturor punctelor terminale ale organizației, inclusiv desktopuri, laptopuri, tablete, telefoane mobile și terminale de punct de vânzare

2.1.2 Dispozitivelor personale utilizate în regim „Bring Your Own Device” (BYOD) pentru accesarea aplicațiilor de afaceri sau a datelor

2.1.3 Dispozitivelor de stocare amovibile, precum unități USB și hard diskuri externe

2.1.4 Oricăror sisteme de operare, aplicații pentru puncte terminale sau instrumente de comunicații care rulează pe aceste platforme

**2.2 Se aplică în egală măsură:**

2.2.1 Personalului intern, contractanților, stagiarilor și furnizorilor de servicii administrate (MSP)

2.2.2 Dispozitivelor utilizate la sediu, la distanță sau în regim de muncă hibrid

2.2.3 Punctelor terminale conectate la cloud sau offline care stochează date de afaceri sau date cu caracter personal

**3. Obiective**

3.1 Prevenirea infectării cu malware și a propagării acestuia în sistemele interne, pe dispozitivele utilizatorilor și prin conexiuni externe

3.2 Detectarea și limitarea rapidă a amenințărilor asociate malware-ului prin utilizarea tehnologiilor automatizate de securitate a punctelor terminale și a fluxurilor de escaladare definite

3.3 Asigurarea faptului că numai dispozitive autorizate, securizate și monitorizate sunt utilizate pentru accesarea informațiilor de afaceri

3.4 Stabilirea unor responsabilități clare pentru personal și a unor reguli de comportament pentru utilizatori, pentru a reduce riscul incidentelor asociate malware-ului

3.5 Menținerea unor înregistrări trasabile și verificabile privind detectările de malware, răspunsul aplicat și conformitatea cu politica

3.6 Protejarea datelor cu caracter personal și a datelor de afaceri împotriva compromiterii cauzate de malware prin strategii de apărare în profunzime

**4. Roluri și responsabilități**

**4.1 Director general**

4.1.1 Deține această politică și asigură disponibilitatea resurselor suficiente pentru protecția punctelor terminale

4.1.2 Aprobă software-ul antivirus, instrumentele de gestionare a dispozitivelor mobile și regulile privind accesul terților

4.1.3 Revizuiește rapoartele privind incidentele de malware, sintezele de impact și notificările privind încălcările care implică puncte terminale

**4.2 Furnizorul de suport IT / administratorul IT intern**

4.2.1 Selectează și implementează software antivirus, antimalware și soluții de detectare și răspuns la nivel de punct terminal (EDR)

4.2.2 Se asigură că actualizările sunt aplicate consecvent și că jurnalele sunt păstrate

4.2.3 Răspunde la alertele de malware, izolează sistemele infectate și efectuează remedierea

4.2.4 Aplică controale privind utilizarea dispozitivelor USB și a dispozitivelor externe

[ ... 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 Cerință de revizuire anuală**

9.1.1 Această politică trebuie revizuită formal cel puțin o dată pe an de către Directorul general, în coordonare cu Furnizorul de suport IT și Coordonatorul pentru confidențialitate

**9.2 Actualizări declanșate de evenimente**

**9.2.1 Actualizările politicii trebuie realizate și atunci când:**

9.2.1.1 O nouă amenințare majoră de tip malware sau un focar vizează punctele terminale utilizate de organizație

9.2.1.2 Instrumentele antivirus sau EDR sunt schimbate, modernizate sau înlocuite

9.2.1.3 Un incident de malware relevă puncte slabe în domeniul de aplicare al acestei politici sau în implementarea acesteia

9.2.1.4 Cerințele legale sau de reglementare (de ex., GDPR, DORA, NIS2) sunt actualizate

**9.3 Controlul versiunilor și comunicare**

9.3.1 Toate modificările politicii trebuie documentate cu un număr de versiune, dată și un rezumat al modificărilor

9.3.2 Personalul trebuie notificat cu privire la actualizări, în special dacă acestea modifică cerințele operaționale sau comportamentale

9.3.3 Versiunile anterioare trebuie păstrate în arhiva politicilor timp de cel puțin 3 ani pentru a sprijini auditurile

## 10. Politici conexe și interdependențe

### 10.1 Această politică trebuie implementată împreună cu următoarele politici SME:

10.1.1 P9S – Politica de telemuncă: Asigură aplicarea cerințelor de protecție a punctelor terminale pe dispozitivele utilizate în afara sediului sau în regim hibrid

10.1.2 P12S – Politica de management al activelor: Sprijină evidența și controlul tuturor punctelor terminale, asigurând că sunt utilizate numai dispozitive autorizate și protejate

10.1.3 P17S – Politica privind protecția datelor și confidențialitatea: Consolidează prevenirea malware-ului ca măsură de bază pentru confidențialitate, pentru protejarea datelor cu caracter personal și a datelor sensibile împotriva compromiterii

10.1.4 P22S – Politica de jurnalizare și monitorizare: Stabilește cerințele pentru jurnalizarea evenimentelor de malware și menținerea vizibilității alertelor pentru un răspuns timpuriu

10.1.5 P30S – Politica de răspuns la incidente: Definește pașii de escaladare, limitare și notificare externă dacă malware-ul conduce la compromiterea datelor sau la perturbări operaționale

## 11. Standarde și cadre de referință

### 11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Impune implementarea controalelor operaționale pentru reducerea riscurilor, inclusiv a atacurilor de tip malware

### 11.2 ISO/IEC 27002

11.2.1 Control 8.7 – Detaliază practicile de control al malware-ului, inclusiv antivirus, scanare în timp real, actualizări și instruirea utilizatorilor

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Impune implementarea mecanismelor de protecție împotriva codului malițios la nivelul punctelor terminale

11.3.2 SI-4 – Impune acțiuni de monitorizare, detectare, analiză și răspuns pentru amenințările și alertele la nivelul punctelor terminale

### 11.4 GDPR al UE

11.4.1 Articolul 32(1)(b) – Impune controale tehnice și organizatorice (precum antivirus) pentru protejarea datelor cu caracter personal

11.4.2 Articolul 33 – Impune notificarea încălcării securității datelor atunci când malware-ul compromite integritatea, confidențialitatea sau disponibilitatea datelor

### 11.5 Directiva NIS2 a UE

11.5.1 Articolul 21(2)(d) – Impune măsuri pentru prevenirea și răspunsul la amenințările de tip malware în cadrul entităților esențiale și importante

11.5.2 Articolul 21(2)(e) – Impune strategii stratificate de management al riscurilor de securitate cibernetică, inclusiv protecția punctelor terminale împotriva malware-ului

### 11.6 Regulamentul DORA al UE

11.6.1 Articolul 10(1) – Impune protejarea sistemelor TIC împotriva malware-ului și a altor amenințări ca parte a rezilienței operaționale

11.6.2 Articolul 15 – Impune organizațiilor financiare să verifice protecția împotriva malware-ului la nivelul furnizorilor terți de servicii

**11.7 COBIT 2019**

11.7.1 DSS05.02 – Evidențiază măsurile de protecție pentru apărarea punctelor terminale și a rețelelor împotriva amenințărilor de tip malware

11.7.2 DSS05.04 – Sprijină monitorizarea și alertarea privind evenimentele de securitate asociate malware-ului ca parte a activităților operaționale curente