| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Introduceți aici denumirea entității juridice înregistrate | | | | | | | |
| Numărul documentului:<br>P22S | | | | | Titlul documentului:<br>**Politica de jurnalizare și monitorizare** | | | | | | | |
| 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** |
| | | | |
| | | | |

Aliniată la standardele și reglementările aplicabile

| Standard/reglementare | Clauză/articol | Comentariu |
|---|---|---|
| ISO/IEC 27001:2022 | Clauza 8 | Controale operaționale, inclusiv jurnalizare |
| ISO/IEC 27002:2022 | Controalele 8.15, 8.16, 8.17 | Jurnalizarea evenimentelor, protecția acestora și monitorizarea |
| NIST SP 800-53 Rev.5 | AU-2 până la AU-12, SI-4 | Conținutul și revizuirea jurnalelor de audit, păstrarea, detectarea anomaliilor, alertarea |
| GDPR | Articolele 5(1)(f), 32, 33 | Confidențialitatea și integritatea datelor, măsuri tehnice și notificarea încălcărilor |
| Directiva NIS2 | Articolele 21(2)(d), 23 | Mecanisme de jurnalizare pentru detectarea anomaliilor și raportarea incidentelor în termen de 24 de ore |
| Regulamentul DORA | Articolele 10, 15 | Reziliență operațională digitală, monitorizarea și jurnalizarea furnizorilor de servicii |
| COBIT 2019 | DSS01.03, DSS05.02 | Trasabilitatea activităților și protecție prin jurnalizare și monitorizare |

**1. Scop**

1.1 Prezenta politică stabilește controale obligatorii de jurnalizare și monitorizare pentru a asigura securitatea, responsabilitatea și integritatea operațională a sistemelor IT ale organizației.

1.2 Aceasta definește tipurile de evenimente care trebuie jurnalizate, modul de stocare a jurnalelor, modul în care acestea sunt revizuite, precum și responsabilitățile personalului și ale furnizorilor de servicii.

1.3 Jurnalizarea și monitorizarea sprijină detectarea amenințărilor, conformitatea cu cerințele de reglementare, răspunsul la incidente și analiza criminalistică.

1.4 Prezenta politică permite organizației să îndeplinească cerințele privind controalele operaționale din ISO/IEC 27001 și sprijină pregătirea continuă pentru audit, încrederea clienților și conformitatea cu GDPR, NIS2 și DORA.

**2. Domeniu de aplicare**

**2.1 Prezenta politică se aplică tuturor sistemelor și utilizatorilor din cadrul organizației, inclusiv:**

2.1.1 stații de lucru, laptopuri, servere, firewall-uri, switch-uri, routere și puncte de acces wireless

2.1.2 servicii cloud utilizate pentru activitățile operaționale ale organizației (de exemplu, e-mail, stocare de fișiere, backup, instrumente de colaborare)

2.1.3 funcții de jurnalizare din software-ul antivirus, aplicații, sisteme de operare și echipamente de rețea

2.1.4 toți angajații, contractanții și furnizorii de servicii administrate (MSP) care utilizează sau administrează sisteme

2.1.5 orice locație în care sunt utilizate sisteme IT ale companiei, inclusiv medii la distanță, hibride sau de tip BYOD

2.2 Politica se aplică, de asemenea, jurnalelor generate de servicii terțe în cazurile în care organizația are acces administrativ sau drepturi contractuale de audit.

**3. Obiective**

3.1 Asigurarea jurnalizării activităților sistemelor, inclusiv autentificarea, modificările de configurație, accesul la date sensibile și alertele de securitate

3.2 Menținerea unor jurnale securizate și exacte pentru detectarea încălcărilor de politică, a erorilor de sistem sau a acțiunilor neautorizate

3.3 Asigurarea unei revizuiri prompte a jurnalelor în timpul incidentelor, investigațiilor și auditurilor

3.4 Sprijinirea sincronizării timpului pentru a asigura integritatea și corelarea datelor din jurnale

3.5 Protejarea jurnalelor împotriva alterării, pierderii sau ștergerii premature

3.6 Îndeplinirea obligațiilor legale și de reglementare privind responsabilitatea sistemelor, trasabilitatea și răspunsul la încălcări

**4. Roluri și responsabilități**

**4.1 Director general**

4.1.1 Aprobă prezenta politică și asigură implementarea acesteia în toate sistemele de business

4.1.2 Revizuiește alertele cu severitate ridicată și constatările grave de audit raportate de funcțiile IT sau de protecția datelor

4.1.3 Aprobă excepțiile în care jurnalizarea sau păstrarea nu pot fi impuse din motive tehnice

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

4.2.1 Implementează și configurează jurnalizarea pentru sisteme de operare, dispozitive de rețea, instrumente antivirus și aplicații critice

4.2.2 Se asigură că jurnalele sunt păstrate, salvate prin backup și protejate împotriva modificării

4.2.3 Revizuiește jurnalele conform unui calendar stabilit și investighează activitățile suspecte sau neautorizate

4.2.4 Menține sisteme de alertare care semnalează comportamente anormale sau indicatori de compromitere

[ ... 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 Prezenta politică trebuie revizuită cel puțin anual de Directorul general, cu sprijinul Furnizorului de suport IT și al Coordonatorului de confidențialitate.

**9.2 Declanșatoare ale revizuirii**

**9.2.1 Revizuirile neplanificate trebuie efectuate ca răspuns la:**

9.2.1.1 constatări legate de jurnalizare rezultate din audituri interne sau externe

9.2.1.2 incidente de securitate în care jurnalele au lipsit, au fost corupte sau au fost insuficiente

9.2.1.3 modificări semnificative ale infrastructurii IT (de exemplu, migrarea către platforme cloud de jurnalizare)

9.2.1.4 actualizări ale obligațiilor legale sau de reglementare (de exemplu, GDPR, NIS2, DORA)

**9.3 Controlul versiunilor**

9.3.1 Toate modificările aduse prezentei politici trebuie înregistrate împreună cu numărul versiunii, data și sinteza revizuirilor

9.3.2 Versiunile anterioare trebuie arhivate și păstrate cel puțin 3 ani

9.3.3 Politicile actualizate trebuie comunicate părților interesate afectate, în special celor care au acces la nivel de sistem

## 10. Politici conexe și interdependențe

### 10.1 Prezenta politică susține în mod direct și este susținută de următoarele politici SME privind securitatea informațiilor:

10.1.1 P17S – Politica de protecție a datelor și confidențialitate: asigură că datele din jurnale care conțin informații cu caracter personal sunt gestionate cu măsuri de protecție privind integritatea, păstrarea și accesul, în conformitate cu cerințele GDPR.

10.1.2 P21S – Politica de securitate a rețelei: oferă baza pentru colectarea jurnalelor referitoare la firewall-uri, acces wireless, VPN-uri și monitorizarea segmentării.

10.1.3 P24S – Politica de dezvoltare securizată: asigură că jurnalele aplicațiilor (de exemplu, pentru tentative de autentificare, erori și excepții) sunt integrate în proiectarea și operarea software-ului.

10.1.4 P30S – Politica de răspuns la incidente: se bazează pe date de jurnal exacte și complete pentru a detecta, analiza și trata evenimentele de securitate a informațiilor.

10.1.5 P23S – Politica de sincronizare a timpului: asigură marcaje temporale consecvente și trasabile în toate sistemele, permițând corelarea jurnalelor în timpul investigațiilor.

## 11. Standarde și cadre de referință

### 11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – impune implementarea controalelor operaționale pentru atenuarea riscurilor de securitate a informațiilor, inclusiv jurnalizarea.

### 11.2 ISO/IEC 27002

11.2.1 Controlul 8.15 – impune jurnalizarea evenimentelor pentru a sprijini detectarea anomaliilor și responsabilitatea.

11.2.2 Controlul 8.16 – impune protejarea jurnalelor împotriva alterării și accesului neautorizat.

11.2.3 Controlul 8.17 – impune monitorizarea sistemelor pentru activități neobișnuite și confirmarea eficacității controalelor de monitorizare.

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

11.3.1 AU-2 până la AU-12 – acoperă conținutul jurnalelor de audit, revizuirea, păstrarea și alertarea automată.

11.3.2 SI-4 – impune detectarea anomaliilor de sistem și raportarea evenimentelor suspecte.

### 11.4 GDPR

11.4.1 Articolul 5(1)(f) – impune integritatea și confidențialitatea datelor cu caracter personal, ceea ce include jurnalizarea accesului.

11.4.2 Articolul 32 – impune măsuri tehnice și organizatorice pentru asigurarea securității, inclusiv jurnalizare și monitorizare.

11.4.3 Articolul 33 – impune notificarea la timp a încălcărilor, susținută de jurnale care permit analiza cauzei principale.

### 11.5 Directiva NIS2

11.5.1 Articolul 21(2)(d) – impune mecanisme de jurnalizare care detectează anomalii și oferă suport pe durata investigațiilor incidentelor.

11.5.2 Articolul 23 – impune raportarea incidentelor în termen de 24 de ore, ceea ce depinde de date de jurnal exacte și disponibile la timp.

**11.6 Regulamentul DORA**

11.6.1 Articolul 10 – impune reziliență operațională digitală, inclusiv trasabilitatea incidentelor legate de TIC prin jurnalizare.

11.6.2 Articolul 15 – impune monitorizarea furnizorilor de servicii, inclusiv drepturi de acces la jurnale și de revizuire.

**11.7 COBIT 2019**

11.7.1 DSS01.03 – impune trasabilitatea activității sistemelor prin jurnalizare și monitorizare.

11.7.2 DSS05.02 – tratează jurnalizarea ca un control esențial pentru protecția împotriva malware-ului și a altor activități neautorizate.