					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P22					Titlul documentului: **Politica de jurnalizare și monitorizare**							
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**

1. Scop

1.1 Scopul acestei politici este de a stabili cerințe clare și obligatorii pentru generarea, protejarea, revizuirea și analiza jurnalelor care înregistrează evenimente-cheie de sistem și de securitate în întregul mediu IT al organizației.

1.2 Jurnalizarea și monitorizarea sunt esențiale pentru detectarea anomaliilor, răspunsul la amenințări, investigațiile criminalistice, pregătirea pentru audit și conformitatea juridică. Această politică asigură că toate evenimentele generate de sisteme sunt înregistrate în mod corespunzător, păstrate și corelate cu acuratețe pe baza unei sincronizări corecte a timpului.

1.3 Această politică este esențială pentru susținerea clauzei 8.1 din ISO/IEC 27001 și a controalelor din Anexa A 8.15 (Jurnalizare), 8.16 (Monitorizare) și 8.17 (Sincronizarea ceasului) și este aliniată direct la obligațiile de reglementare prevăzute de GDPR, NIS2, DORA și COBIT 2019.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor sistemelor, serviciilor și mediilor care stochează, prelucrează sau transmit date aflate în domeniul de aplicare al Sistemului de management al securității informației (SMSI), inclusiv:

2.1.1 infrastructură on-premises, servicii cloud (de ex., IaaS, PaaS, SaaS) și medii hibride

2.1.2 sisteme de operare, baze de date, aplicații și echipamente de rețea

2.1.3 sisteme de securitate, precum platforme SIEM, firewall-uri, platforme de detectare și răspuns la nivel de endpoint (EDR), concentratoare VPN și furnizori de identitate

2.2 Următoarele părți interesate sunt incluse în domeniul de aplicare:

2.2.1 utilizatori interni cu privilegii de sistem sau administrative

2.2.2 personal de infrastructură și operațiuni IT

2.2.3 echipele Centrului de Operațiuni de Securitate (SOC) și de detecție a amenințărilor

2.2.4 dezvoltatori software și proprietari de aplicații

2.2.5 furnizori terți de servicii care administrează sisteme care generează jurnale

3. Obiective

3.1 Asigurarea faptului că toate sistemele critice generează jurnale privind evenimentele de securitate și înregistrări ale activităților de sistem, păstrate în conformitate cu cerințele de reglementare, juridice și contractuale.

3.2 Definirea tipurilor minime de evenimente și a conținutului minim al jurnalelor necesare pentru detectarea activităților neautorizate, urmărirea acțiunilor utilizatorilor și susținerea investigațiilor criminalistice.

3.3 Impunerea unor măsuri de protecție pentru a preveni alterarea jurnalelor, ștergerea neautorizată sau accesul necontrolat la datele din jurnale.

3.4 Instituirea unor sisteme centralizate de jurnalizare și alertare (de ex., SIEM) pentru agregarea, corelarea și escaladarea activităților suspecte în timp aproape real.

3.5 Asigurarea sincronizării ceasurilor sistemelor pentru a permite corelarea exactă între sisteme și analiza incidentelor.

3.6 Susținerea îmbunătățirii continue și a conformității prin integrarea monitorizării jurnalelor cu procesele de audit, management al riscurilor și management al incidentelor.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține această politică și asigură alinierea acesteia la profilul de risc al securității organizației, la cerințele de audit și la obligațiile SMSI.

4.1.2 Aprobă domeniul de aplicare al jurnalizării pentru sistemele reglementate sau cu risc ridicat și exercită supravegherea raportării privind conformitatea.

4.2 Managerul Centrului de Operațiuni de Securitate (SOC)

4.2.1 Operează și menține platformele centralizate de management al jurnalelor (de ex., SIEM).

4.2.2 Definește regulile de agregare a jurnalelor, pragurile de alertare și căile de escaladare pentru triajul incidentelor.

4.2.3 Revizuiește rapoartele zilnice și se asigură că anomaliile sunt analizate, documentate și escaladate, după caz.

[... 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 mai devreme ca răspuns la:

9.1.1 modificări majore în arhitectura sistemelor sau în infrastructura de jurnalizare (de ex., migrare SIEM)

9.1.2 revizuiri ale cerințelor de reglementare privind jurnalizarea (de ex., cerințe NIS2, DORA privind jurnalizarea)

9.1.3 constatări rezultate din audituri sau analize post-incident

9.1.4 riscuri emergente care impun monitorizare consolidată (de ex., amenințări interne, compromiterea lanțului de aprovizionare)

9.2 Procesul de revizuire este coordonat de Managerul Centrului de Operațiuni de Securitate (SOC), în colaborare cu CISO, funcția de management al riscurilor, conformitatea și echipele de infrastructură IT.

9.3 Modificările aprobate trebuie să facă obiectul controlului versiunilor în registrul de control al documentelor SMSI și să fie comunicate către:

9.3.1 toate părțile interesate cu responsabilități privind mentenanța sistemelor de jurnalizare

9.3.2 proprietarii de aplicații și de sisteme

9.3.3 furnizorii terți cu responsabilități privind telemetria sau integrarea cu SIEM

9.4 Toate versiunile înlocuite trebuie arhivate în condiții de securitate, cu acces restricționat la responsabilii autorizați ai SMSI în scopuri de audit și juridice.

10. Politici conexe și interdependențe

10.1 P1 – Politica de securitate a informației. Stabilește angajamentul de bază pentru protejarea sistemelor și datelor, în cadrul căruia jurnalizarea și monitorizarea acționează ca mecanisme critice de detecție și răspuns.

10.2 P4 – Politica de control al accesului. Asigură că accesul privilegiat, autentificările utilizatorilor și evenimentele de autorizare sunt capturate în jurnale și monitorizate pentru identificarea utilizării abuzive sau a comportamentului anormal.

10.3 P5 – Politica de management al schimbărilor. Impune jurnalizarea modificărilor de sistem, a implementării patch-urilor și a actualizărilor de configurație care pot introduce riscuri sau modificări neautorizate.

10.4 P21 – Politica de securitate a rețelei. Impune jurnalizarea la nivel de rețea (de ex., jurnale de firewall, alerte IDS/IPS, activitate VPN) și integrarea cu SIEM pentru vizibilitate asupra anomaliilor de trafic și protecției perimetrului.

10.5 P23 – Politica de sincronizare a timpului. Impune consecvența ceasului între sisteme, esențială pentru o jurnalizare fiabilă și pentru corelarea evenimentelor de securitate în medii multiple.

10.6 P30 – Politica de răspuns la incidente. Se bazează pe datele din jurnale și pe mecanismele de alertare pentru a identifica, investiga și gestiona incidente de securitate a informației, păstrând totodată artefactele criminalistice pentru analiza post-incident.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Planificare și control operațional: impune controale pentru monitorizarea operațiunilor și protejarea împotriva accesului neautorizat și a utilizării abuzive a sistemelor.

11.2 ISO/IEC 27002:2022 – Controalele 8.15, 8.16, 8.17

11.2.1 Definește cerințe detaliate de jurnalizare, inclusiv ce evenimente trebuie înregistrate, cum trebuie protejate și analizate jurnalele și cum trebuie asigurată fiabilitatea marcajului temporal între sisteme.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 până la AU-12: acoperă selectarea evenimentelor, jurnalizarea, protecția, revizuirea auditului, răspunsul la eșecurile de audit și păstrarea înregistrărilor de audit.

11.3.2 SI-4 – Monitorizarea sistemului: impune monitorizarea activă a sistemului cu alerte bazate pe activitate anormală.

11.3.3 SC-45 – Sincronizarea timpului sistemului: consolidează acuratețea timpului pentru trasabilitatea evenimentelor și corelarea incidentelor.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 32 – Securitatea prelucrării: impune controale tehnice precum jurnalizarea și monitorizarea pentru a asigura securitatea și responsabilitatea, în special pentru accesul la date cu caracter personal.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(e): impune sisteme de jurnalizare și monitorizare a evenimentelor pentru detectarea rapidă și răspunsul la incidente de securitate.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: impune mecanisme pentru detectarea activităților anormale, jurnalizarea incidentelor și păstrarea datelor criminalistice.

11.6.2 Articolul 11 – Testarea planurilor de continuitate a activității (BCP/DRP): evidențiază continuitatea monitorizării și validarea disponibilității jurnalelor în timpul perturbărilor operaționale.

11.7 COBIT 2019

11.7.1 DSS01.05 – Gestionarea jurnalelor de securitate: impune implementarea capabilităților de jurnalizare pentru întreaga infrastructură critică.

11.7.2 DSS05.04 – Monitorizarea evenimentelor de securitate: impune monitorizarea și analiza în timp real a jurnalelor pentru detectarea și răspunsul la evenimente.

11.7.3 MEA03 – Măsurarea, evaluarea și analiza conformității: impune revizuirea periodică a practicilor de jurnalizare și alinierea la obiectivele de control.