					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P23					Titlul documentului: **Politica privind sincronizarea timpului**							
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	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
GDPR al UE	Articolul 32	-
Directiva NIS2 a UE	Articolul 21(2)(e)	-
Regulamentul DORA al UE	Articolele 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Scop

1.1 Scopul acestei politici este de a asigura că toate sistemele, aplicațiile, dispozitivele și serviciile cloud ale organizației mențin setări de timp consecvente și exacte prin sincronizarea cu surse de timp desemnate și de încredere.

1.2 Sincronizarea exactă a timpului este esențială pentru jurnalizare fiabilă, comunicații securizate, trasabilitate în audit, răspuns la incidente și investigații criminalistice. Nealinierea temporală poate conduce la jurnale care nu pot fi corelate, autentificări eșuate și raportări de reglementare incomplete.

1.3 Această politică sprijină controlul 8.17 din Anexa A la ISO/IEC 27001 și standardele internaționale conexe prin impunerea acurateței timpului și a detectării derivei ceasului în întregul parc IT al organizației.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor:

2.1.1 tuturor componentelor de infrastructură, inclusiv serverelor, stațiilor de lucru, echipamentelor de rețea, firewall-urilor și sistemelor din Internetul obiectelor (IoT)

2.1.2 mediilor virtuale și cloud (de exemplu, AWS, Azure, Google Cloud)

2.1.3 tuturor sistemelor care participă la jurnalizare, autentificare, prelucrarea tranzacțiilor sau corelarea evenimentelor de securitate

2.1.4 angajaților interni, contractorilor și furnizorilor terți de servicii care au responsabilități asupra sistemelor sensibile la timp

2.2 În domeniul de aplicare sunt incluse toate sistemele care generează sau consumă înregistrări cu marcaj temporal, cum ar fi intrări în jurnale, alerte, înregistrări ale activității utilizatorilor sau probe criminalistice.

3. Obiective

3.1 Să definească o arhitectură consecventă și centralizată pentru sincronizarea timpului, utilizând surse NTP aprobate sau echivalente.

3.2 Să asigure că toate sistemele își sincronizează ceasurile la intervale definite și că orice derivă este detectată și corectată automat sau cu intervenție minimă.

3.3 Să mențină acuratețea ceasului în medii hibride, on-premises și cloud, pentru a permite:

3.3.1 corelarea fiabilă a evenimentelor și răspunsul la incidente

3.3.2 conformitatea cu reglementările și standardele, precum ISO 27001, GDPR, NIS2 și DORA

3.3.3 protecția împotriva atacurilor de tip replay și a eșecurilor de autentificare bazate pe timp

3.4 Să stabilească roluri clare, proceduri de tratare a excepțiilor și mecanisme de audit pentru a asigura aplicarea acestei politici.

3.5 Să asigure că anomaliile legate de timp sunt jurnalizate, generează alerte și sunt escaladate atunci când depășesc toleranțele stabilite.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține această politică și asigură alinierea cu controalele operaționale ale Sistemului de management al securității informației (SMSI) și cu cerințele de reglementare.

4.1.2 Aprobă selecția surselor de timp la nivelul organizației și validează procesele de raportare privind sincronizarea timpului.

4.2 Managerul serviciilor de infrastructură / responsabilul cu ingineria de rețea

4.2.1 Menține serverele NTP primare și secundare ale organizației sau configurația surselor de timp desemnate.

4.2.2 Se asigură că toate dispozitivele conectate la rețea și instanțele virtuale sincronizează timpul la intervale corespunzătoare.

4.2.3 Monitorizează jurnalele de sincronizare a timpului, alertele privind deriva ceasului și condițiile de eroare.

[... 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 în următoarele condiții:

9.1.1 detectarea unor exploituri bazate pe timp sau a unor eșecuri de jurnalizare

9.1.2 modificări ale infrastructurii de timp de bază (de exemplu, noi servere NTP la nivelul organizației sau actualizări de protocol)

9.1.3 neconcordanțe privind deriva timpului pe platformele cloud sau modificări ale serviciilor regionale

9.1.4 constatări post-incident care identifică nealinierea timpului drept factor contribuitor

9.2 Revizuirea trebuie coordonată de responsabilul de infrastructură, cu contribuția necesară din partea SOC, a securității aplicațiilor și a părților interesate din zona de conformitate.

9.3 Revizuirile trebuie documentate în Registrul documentelor al SMSI și comunicate părților interesate interne și terțe afectate.

9.4 Versiunile istorice ale politicii trebuie arhivate în mod securizat, supuse controlului versiunilor și puse la dispoziție pentru solicitări de audit de conformitate sau audit juridic.

10. Politici conexe și interdependențe

10.1 P1 – Politica de securitate a informației. Stabilește mandatul general pentru asigurarea integrității și trasabilității tuturor sistemelor informatice, pentru care acuratețea timpului reprezintă un element fundamental.

10.2 P5 – Politica de management al schimbărilor. Reglementează modificările configurațiilor de sistem, inclusiv ajustările surselor de timp, asigurând documentarea corespunzătoare, testarea și existența planurilor de revenire.

10.3 P22 – Politica de jurnalizare și monitorizare. Depinde în mod direct de timpul sincronizat pentru a asigura secvențierea evenimentelor, corelarea jurnalelor și integritatea investigațiilor incidentelor în sisteme diverse.

10.4 P30 – Politica de răspuns la incidente. Se bazează pe marcaje temporale exacte pentru investigații criminalistice, cronologii ale incidentelor și dovezi din lanțul de custodie. Timpul inexact compromite credibilitatea rapoartelor de incident.

10.5 P20 – Politica privind protecția endpoint-urilor / politica antimalware. Impune alertare cu timp exact și analiză comportamentală pentru a detecta propagarea malware-ului, mișcarea laterală și anomaliile de acces.

10.6 P6 – Politica de management al riscurilor. Definește desincronizarea drept risc operațional și criminalistic potențial, impunând controalele definite în această politică pentru atenuarea impactului.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Planificare și control operațional: impune integrarea unor controale tehnice exacte, precum ceasurile de sistem sincronizate, pentru o execuție operațională fiabilă.

11.2 ISO/IEC 27002:2022 – Control 8

11.2.1 Consolidează cerința privind acuratețea ceasului și impune consecvența timpului de sistem la nivelul organizației pentru a facilita compararea jurnalelor, investigațiile și validarea securizată a tranzacțiilor.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Sincronizarea timpului sistemului: impune sincronizarea timpului utilizând surse autorizate la nivelul tuturor componentelor aflate în limitele sistemului.

11.3.2 AU-8 – Marcaje temporale: asigură marcarea temporală corectă a evenimentelor și oferă trasabilitate pentru audit și răspuns la incidente.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 32 – Securitatea prelucrării: deși nu menționează explicit timpul, impune utilizarea unor măsuri tehnice adecvate — inclusiv piste de audit și jurnale — care depind în mod inerent de marcaje temporale sincronizate pentru validitate și integritate.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(e): impune capabilități de jurnalizare și detecție care presupun o sincronizare exactă a timpului pentru corelarea între sisteme și răspunsul în timp util.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: impune telemetrie exactă a sistemelor pentru monitorizarea riscurilor și detectarea anomaliilor, ceea ce depinde de sincronizarea precisă a ceasului.

11.6.2 Articolul 10 – Continuitatea activității TIC: impune controale care asigură integritatea sistemului în timpul perturbărilor, inclusiv înregistrări ale evenimentelor aliniate temporal.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorizarea evenimentelor de securitate: impune integritatea marcajelor temporale pentru analiza eficace a jurnalelor și detectarea amenințărilor.

11.7.2 MEA03 – Măsurarea, evaluarea și analiza conformității: sincronizarea timpului sprijină auditarea corectă a conformității și ciclurile de raportare.