					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P23S					Titlul documentului: **Politica de sincronizare a 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	Cerințe de control relevante
ISO/IEC 27002:2022	Controlul 8	Funcționare sincronizată a sistemelor
NIST SP 800-53 Rev.5	SC-45, AU-8	NTP de încredere și acuratețea marcajelor temporale din jurnale
GDPR al UE	Articolele 5(1)(d), 32	Acuratețe, responsabilitate și integritate în prelucrarea datelor cu caracter personal prin utilizarea unor marcaje temporale sincronizate
Directiva NIS2 a UE	Articolul 21(2)(d)	Capabilități de monitorizare și detectare susținute de jurnale sincronizate
Regulamentul DORA al UE	Articolele 10, 15	Reziliență operațională și înregistrări tehnice exacte
COBIT 2019	DSS05.02, MEA03	Evenimente marcate temporal și monitorizare bazată pe dovezi

1. Scop

1.1 Prezenta politică stabilește controale obligatorii pentru menținerea unui timp precis și sincronizat în toate sistemele care stochează, transmit sau prelucrează datele organizației.

1.2 Sincronizarea timpului este esențială pentru asigurarea trasabilității jurnalelor de sistem, corelarea exactă a incidentelor de securitate și utilizarea fiabilă a probelor în cadrul analizelor criminalistice sau al revizuirilor juridice.

1.3 Organizația impune sincronizarea automată a timpului ca cerință de bază pentru integritatea auditului, răspunsul la incidente și conformitatea cu cerințele ISO 27001, GDPR, DORA și NIS2.

1.4 Prezenta politică asigură utilizarea unor surse de timp de încredere de către toate sistemele, previne suprascrierea manuală a setărilor de timp și impune corectarea la timp a derivei ceasului.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică următoarelor:

2.1.1 tuturor sistemelor și dispozitivelor deținute de companie, inclusiv servere, sisteme desktop, laptopuri, dispozitive mobile, firewall-uri, routere și mașini virtuale;

2.1.2 infrastructurii de la distanță și infrastructurii găzduite în cloud utilizate în activitățile operaționale ale organizației (de exemplu, AWS, Microsoft 365, platforme SaaS);

2.1.3 sistemelor care generează sau stochează jurnale de evenimente, înregistrări de autentificare sau piste de audit;

2.1.4 tuturor angajaților, contractanților, furnizorilor sau furnizorilor de suport IT responsabili pentru configurarea sau mentenanța acestor sisteme.

2.2 Politica se aplică, de asemenea, punctelor terminale utilizate în cadrul programului adu propriul dispozitiv (BYOD) pentru accesarea sistemelor organizației, cu condiția ca respectivele puncte terminale să stocheze sau să genereze date relevante pentru audit.

3. Obiective

3.1 Asigurarea faptului că toate sistemele critice sincronizează automat timpul utilizând servere Network Time Protocol (NTP) de încredere sau mecanisme echivalente puse la dispoziție de furnizorii de servicii cloud.

3.2 Prevenirea discrepanțelor de timp care ar putea compromite fiabilitatea sau corelarea jurnalelor de sistem în timpul auditurilor sau al investigațiilor de securitate.

3.3 Permiterea detectării și corectării la timp a derivei de timp care depășește pragurile acceptabile.

3.4 Menținerea marcării temporale consecvente în toate mediile (on-premises, în cloud și la distanță).

3.5 Îndeplinirea cerințelor tehnice și juridice privind integritatea, trasabilitatea și nerepudierea înregistrărilor și evenimentelor.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Aprobă prezenta politică și asigură conformitatea la nivelul organizației.

4.1.2 Asigură supravegherea revizuirilor periodice privind acuratețea timpului la nivel de sistem și a lacunelor de implementare.

4.1.3 Aprobă excepțiile de la sincronizarea automată a timpului, atunci când acestea sunt justificate și documentate.

4.2 Furnizorul de suport IT / rolul IT intern

4.2.1 Configurează sincronizarea timpului pentru toate sistemele deținute sau administrate de companie.

4.2.2 Verifică zilnic sau conform planificării că sincronizarea funcționează corect.

4.2.3 Investighează și remediază evenimentele de derivă a timpului, eșecurile de sincronizare sau problemele de acces la NTP.

4.2.4 Documentează starea sincronizării timpului ca parte a verificărilor lunare privind starea sistemelor.

[... 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 programată

9.1.1 Prezenta politică trebuie revizuită anual de Directorul general, furnizorul de suport IT și responsabilul cu protecția datelor.

9.1.2 Toate jurnalele și rapoartele privind starea conformității cu cerințele de sincronizare a timpului trebuie luate în considerare în cadrul revizuirii.

9.2 Actualizări declanșate de evenimente

9.2.1 Prezenta politică trebuie actualizată dacă:

9.2.1.1 o defecțiune a sistemului conduce la o derivă semnificativă a timpului;

9.2.1.2 un audit identifică deficiențe în sincronizarea timpului;

9.2.1.3 organizația adoptă medii noi în cloud, hibride sau de virtualizare;

9.2.1.4 modificările legale sau de reglementare introduc noi cerințe privind integritatea timpului.

9.3 Controlul versiunilor și comunicare

9.3.1 Toate actualizările trebuie să fie supuse controlului versiunilor și datate.

9.3.2 Schimbările majore trebuie comunicate întregului personal tehnic.

9.3.3 Versiunile anterioare trebuie păstrate timp de 3 ani în scop de audit.

10. Politici conexe și interdependențe

10.1 Prezenta politică trebuie aplicată împreună cu următoarele politici SME:

10.1.1 P22S – Politica de jurnalizare și monitorizare: Asigură marcarea temporală consecventă a jurnalelor pentru trasabilitate și corelare criminalistică.

10.1.2 P30S – Politica de răspuns la incidente: Se bazează pe acuratețea marcajelor temporale pentru reconstituirea incidentelor, stabilirea cronologiilor și susținerea deciziilor de notificare.

10.1.3 P17S – Politica de protecție a datelor și confidențialitate: Asigură că jurnalele de acces și cronologiile de gestionare a datelor care implică date cu caracter personal sunt exacte și pot fi susținute în temeiul GDPR.

10.1.4 P12S – Politica de management al activelor: Sprijină identificarea sistemelor care necesită sincronizare, în special a dispozitivelor mobile și de la distanță.

10.1.5 P26S – Politica de securitate a terților și furnizorilor: Asigură, prin clauze contractuale, că furnizorii care accesează sau jurnalizează date pentru organizație respectă practici de sincronizare a timpului.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:

11.1.1 Clauza 8.1 – Impune implementarea controalelor necesare pentru operațiuni securizate, inclusiv jurnalizare și marcare temporală.

11.2 ISO/IEC 27002:

11.2.1 Controlul 8.17 – Recomandă timp sincronizat pentru toate sistemele care produc jurnale sau funcționează în mod colaborativ.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Impune utilizarea surselor de timp interne sau externe pentru acuratețea marcajelor temporale din jurnale.

11.3.2 SC-45 – Specifică utilizarea surselor NTP de încredere și prevenirea modificărilor manuale ale timpului în sistemele critice.

11.4 GDPR al UE:

11.4.1 Articolul 5(1)(d) – Impune acuratețe și responsabilitate în prelucrarea datelor cu caracter personal, susținute de marcaje temporale sincronizate.

11.4.2 Articolul 32 – Impune măsuri de securitate care asigură integritatea datelor, inclusiv intervale de timp consecvente în jurnalizare.

11.5 Directiva NIS2 a UE:

11.5.1 Articolul 21(2)(d) – Impune capabilități de monitorizare și detectare, susținute de jurnale de sistem sincronizate.

11.6 Regulamentul DORA al UE:

11.6.1 Articolul 10 – Impune reziliență operațională, ceea ce necesită jurnale ale incidentelor TIC trasabile și marcate temporal.

11.6.2 Articolul 15 – Impune furnizorilor de servicii să mențină înregistrări tehnice exacte, inclusiv piste de audit marcate temporal.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Evidențiază importanța integrității marcajelor temporale pentru detectarea și răspunsul la evenimente.

11.7.2 MEA03.01 – Impune monitorizarea performanței bazată pe dovezi, susținută de date exacte sincronizate temporal.