					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P23S					Naslov dokumenta: **Politika sinhronizacije časa**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Ustrezne zahteve glede kontrol
ISO/IEC 27002:2022	Kontrola 8	Sinhronizirano delovanje sistemov
NIST SP 800-53 Rev.5	SC-45, AU-8	Zaupanja vreden NTP in natančnost časovnih žigov dnevnikov
Uredba EU GDPR	Člena 5(1)(d), 32	Točnost, odgovornost in celovitost pri obdelavi osebnih podatkov s sinhroniziranimi časovnimi žigi
Direktiva EU NIS2	Člen 21(2)(d)	Zmožnosti spremljanja in zaznavanja, podprte s sinhroniziranimi dnevniki
Uredba EU DORA	Člena 10, 15	Operativna odpornost in natančne tehnične evidence
COBIT 2019	DSS05.02, MEA03	Časovno označeni dogodki in spremljanje na podlagi dokazov

1. Namen

1.1 Ta politika določa obvezne kontrole za vzdrževanje točnega in sinhroniziranega časa v vseh sistemih, ki hranijo, prenašajo ali obdelujejo podatke organizacije.

1.2 Sinhronizacija časa je bistvena za zagotavljanje sledljivosti sistemskih dnevnikov, natančne korelacije varnostnih incidentov ter zanesljivosti dokaznega gradiva pri forenzični analizi ali pravnem pregledu.

1.3 Organizacija uveljavlja samodejno sinhronizacijo časa kot temeljno zahtevo za celovitost revizijske sledi, odzivanje na incidente in regulativno skladnost v skladu z ISO 27001, GDPR, DORA in NIS2.

1.4 Ta politika zagotavlja, da vsi sistemi uporabljajo zaupanja vredne časovne vire, preprečuje ročne spremembe časovnih nastavitev in zahteva pravočasno odpravo odstopanj sistemske ure.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse sisteme in naprave v lasti podjetja, vključno s strežniki, namiznimi računalniki, prenosniki, mobilnimi napravami, požarnimi zidovi, usmerjevalniki in navideznimi stroji,

2.1.2 oddaljeno infrastrukturo in infrastrukturo v oblaku, ki se uporablja pri poslovanju (npr. AWS, Microsoft 365, platforme SaaS),

2.1.3 sisteme, ki ustvarjajo ali hranijo dnevnike dogodkov, evidence avtentikacije ali revizijsko sled,

2.1.4 vse zaposlene, pogodbene izvajalce, dobavitelje ali ponudnike IT-podpore, ki so odgovorni za konfiguriranje ali vzdrževanje teh sistemov.

2.2 Ta politika se uporablja tudi za končne točke v okviru uporabe lastnih naprav, ki se uporabljajo za dostop do poslovnih sistemov, če te končne točke hranijo ali ustvarjajo podatke, pomembne za revizijo.

3. Cilji

3.1 Zagotoviti, da vsi kritični sistemi samodejno sinhronizirajo čas z uporabo zaupanja vrednih strežnikov protokola Network Time Protocol (NTP) ali enakovrednih mehanizmov ponudnikov storitev v oblaku.

3.2 Preprečiti časovna neskladja, ki bi lahko ogrozila zanesljivost ali korelacijo sistemskih dnevnikov med revizijami ali varnostnimi preiskavami.

3.3 Omogočiti pravočasno zaznavanje in odpravo odstopanj časa nad sprejemljivimi pragovi.

3.4 Zagotoviti dosledno časovno označevanje v vseh okoljih (na lokaciji, v oblaku in pri oddaljenem dostopu).

3.5 Izpolniti tehnične in pravne zahteve glede celovitosti, sledljivosti in nezanikanja zapisov ter dogodkov.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 odobri to politiko in zagotavlja skladnost na ravni organizacije,

4.1.2 nadzira periodične preglede točnosti časa na ravni sistemov in vrzeli pri izvajanju,

4.1.3 odobri izjeme od samodejne sinhronizacije časa, kadar so utemeljene in dokumentirane.

4.2 Ponudnik IT-podpore / notranja IT-funkcija

4.2.1 konfigurira sinhronizacijo časa za vse sisteme v lasti podjetja ali sisteme, ki jih podjetje upravlja,

4.2.2 preverja, da dnevna ali načrtovana sinhronizacija deluje pravilno,

4.2.3 preiskuje in odpravlja odstopanja časa, neuspele sinhronizacije ali težave z dostopom do NTP,

4.2.4 dokumentira stanje sinhronizacije časa kot del mesečnih pregledov stanja sistemov.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Načrtovani pregled

9.1.1 To politiko morajo letno pregledati generalni direktor, ponudnik IT-podpore in koordinator za zasebnost.

9.1.2 V okviru pregleda je treba upoštevati vse dnevnike in poročila o stanju skladnosti sinhronizacije časa.

9.2 Posodobitve na podlagi sprožilcev

9.2.1 Ta politika mora biti posodobljena, če:

9.2.1.1 okvara sistema povzroči pomembno odstopanje časa,

9.2.1.2 revizija razkrije pomanjkljivosti pri sinhronizaciji časa,

9.2.1.3 organizacija uvede nova okolja v oblaku, hibridna okolja ali virtualizacijska okolja,

9.2.1.4 pravne ali regulativne spremembe uvedejo nove zahteve glede celovitosti časa.

9.3 Nadzor različic in komunikacija

9.3.1 Vse posodobitve morajo imeti številko različice in datum.

9.3.2 O pomembnih spremembah morajo biti obveščeni vsi člani tehničnega osebja.

9.3.3 Prejšnje različice se morajo hraniti 3 leta za podporo reviziji.

10. Povezane politike in povezave

10.1 Ta politika se mora uporabljati skupaj z naslednjimi politikami SME:

10.1.1 P22S – Politika beleženja in spremljanja: zagotavlja dosledno časovno označevanje v dnevnikih za sledljivost in forenzično korelacijo.

10.1.2 P30S – Politika odzivanja na incidente: temelji na točnosti časovnih žigov za rekonstrukcijo incidentov, določanje časovnic in podporo odločitvam o obveščanju.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da so dnevniki dostopa in časovnice ravnanja s podatki, ki vključujejo osebne podatke, točni in zagovorljivi v skladu z GDPR.

10.1.4 P12S – Politika upravljanja sredstev: podpira identifikacijo sistemov, ki zahtevajo sinhronizacijo, zlasti mobilnih in oddaljenih naprav.

10.1.5 P26S – Politika varnosti tretjih oseb in dobaviteljev: pogodbeno zagotavlja, da dobavitelji, ki za organizacijo dostopajo do podatkov ali jih beležijo, uporabljajo usklajene časovne prakse.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:

11.1.1 Klavzula 8.1 – zahteva uvedbo kontrol, potrebnih za varno delovanje, vključno z beleženjem in časovnim označevanjem.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 8.17 – priporoča sinhroniziran čas za vse sisteme, ki ustvarjajo dnevnike ali delujejo usklajeno z drugimi sistemi.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – zahteva uporabo notranjih ali zunanjih časovnih virov za zagotavljanje natančnosti časovnih žigov dnevnikov.

11.3.2 SC-45 – določa uporabo zaupanja vrednih virov NTP in preprečevanje ročnih sprememb časa v kritičnih sistemih.

11.4 Uredba EU GDPR:

11.4.1 Člen 5(1)(d) – zahteva točnost in odgovornost pri obdelavi osebnih podatkov, podprto s sinhroniziranimi časovnimi žigi.

11.4.2 Člen 32 – zahteva varnostne ukrepe za zagotavljanje celovitosti podatkov, kar vključuje dosledne časovne okvire beleženja.

11.5 Direktiva EU NIS2:

11.5.1 Člen 21(2)(d) – zahteva zmožnosti spremljanja in zaznavanja, podprte s sinhroniziranimi sistemskimi dnevniki.

11.6 Uredba EU DORA:

11.6.1 Člen 10 – zahteva operativno odpornost, kar vključuje sledljive dnevnike incidentov IKT s časovnimi žigi.

11.6.2 Člen 15 – zahteva, da ponudniki storitev vzdržujejo natančne tehnične evidence, vključno z revizijsko sledjo s časovnimi žigi.

11.7 COBIT 2019:

11.7.1 DSS05.02 – poudarja celovitost časovnih žigov za zaznavanje in odzivanje na dogodke.

11.7.2 MEA03.01 – zahteva spremljanje uspešnosti na podlagi dokazov, podprto z natančnimi časovno sinhroniziranimi podatki.