					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P23					Naziv dokumenta: **Politika sinkronizacije vremena**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađenost sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	-
ISO/IEC 27002:2022	Kontrola 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
GDPR EU	Članak 32	-
Direktiva EU NIS2	Članak 21(2)(e)	-
Uredba EU DORA	Članci 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Svrha

1.1 Svrha ove politike jest osigurati da svi sustavi, aplikacije, uređaji i usluge u oblaku unutar organizacije održavaju dosljedne i točne postavke vremena sinkronizacijom s određenim i pouzdanim izvorima vremena.

1.2 Točna sinkronizacija vremena ključna je za pouzdano bilježenje i nadzor, sigurnu komunikaciju, revizijsku sljedivost, odgovor na incidente i forenzičke istrage. Neusklađeno vrijeme može dovesti do nepovezanih dnevničkih zapisa, neuspjele autentikacije i nepotpunog regulatornog izvješćivanja.

1.3 Ova politika podupire kontrolu 8.17 iz Priloga A norme ISO/IEC 27001 i povezane međunarodne standarde tako što osigurava točnost vremena i otkrivanje odstupanja sustavnog vremena u cjelokupnom IT okruženju organizacije.

2. Opseg

2.1 Ova se politika primjenjuje na:

2.1.1 sve infrastrukturne komponente, uključujući poslužitelje, radne stanice, mrežne uređaje, vatrozide i IoT sustave

2.1.2 virtualna okruženja i okruženja u oblaku (npr. AWS, Azure, Google Cloud)

2.1.3 sve sustave koji sudjeluju u bilježenju i nadzoru, autentikaciji, obradi transakcija ili korelaciji sigurnosnih događaja

2.1.4 interne zaposlenike, ugovorne izvođače i pružatelje usluga trećih strana odgovorne za sustave osjetljive na vrijeme

2.2 Sustavi koji generiraju ili koriste zapise s vremenskom oznakom — kao što su dnevnički zapisi, upozorenja, zapisi o aktivnosti korisnika ili forenzički dokazi — smatraju se obuhvaćenima ovom politikom.

3. Ciljevi

3.1 Definirati dosljednu i centraliziranu arhitekturu sinkronizacije vremena uporabom odobrenih NTP izvora ili ekvivalentnog rješenja.

3.2 Osigurati da svi sustavi sinkroniziraju svoje satove u definiranim intervalima te da se svako odstupanje otkrije i ispravi automatski ili uz minimalnu intervenciju.

3.3 Održavati točnost vremena u hibridnim okruženjima, u lokalnim okruženjima i u oblaku kako bi se omogućilo:

3.3.1 pouzdana korelacija događaja i odgovor na incidente

3.3.2 usklađenost sa standardima i regulatornim zahtjevima kao što su ISO 27001, GDPR, NIS2 i DORA

3.3.3 zaštita od replay napada i neuspjeha autentikacije temeljenih na vremenu

3.4 Uspostaviti jasne uloge, postupke za upravljanje iznimkama i revizijske mehanizme radi održavanja provedbe ove politike.

3.5 Osigurati da se anomalije povezane s vremenom evidentiraju, da se za njih generiraju upozorenja i da se eskaliraju kada prekorače dopuštena odstupanja.

4. Uloge i odgovornosti

4.1 Glavni direktor za informacijsku sigurnost (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost s operativnim kontrolama ISMS-a i regulatornim zahtjevima.

4.1.2 Odobrava odabir izvora vremena na razini organizacije i potvrđuje postupke izvješćivanja o sinkronizaciji vremena.

4.2 Voditelj infrastrukturnih usluga / voditelj mrežnog inženjerstva

4.2.1 Održava primarne i sekundarne NTP poslužitelje organizacije ili određenu konfiguraciju izvora vremena.

4.2.2 Osigurava da svi umreženi uređaji i virtualne instance sinkroniziraju vrijeme u odgovarajućim intervalima.

4.2.3 Nadzire dnevničke zapise sinkronizacije vremena, upozorenja o odstupanju vremena i stanja pogrešaka.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ova se politika mora pregledati jednom godišnje ili ranije u sljedećim slučajevima:

9.1.1 otkrivanje iskorištavanja povezanih s vremenom ili neuspjeha bilježenja i nadzora

9.1.2 promjene temeljne infrastrukture vremena (npr. novi organizacijski NTP poslužitelji ili ažuriranja protokola)

9.1.3 odstupanja vremena na platformama u oblaku ili promjene regionalnih usluga

9.1.4 nalazi nakon incidenta koji utvrđuju neusklađenost vremena kao čimbenik koji je pridonio incidentu

9.2 Pregled koordinira voditelj infrastrukture, uz obvezan doprinos Centra sigurnosnih operacija, sigurnosti aplikacija i dionika za usklađenost.

9.3 Izmjene se moraju evidentirati u Registru dokumenata ISMS-a i priopćiti pogođenim internim dionicima i dionicima trećih strana.

9.4 Povijesne verzije politike moraju biti sigurno arhivirane, pod verzijskim nadzorom i dostupne za potrebe usklađenosti ili zahtjeve pravne revizije.

10. Povezane politike i poveznice

10.1 P1 – Politika informacijske sigurnosti. Utvrđuje nadređeni mandat za osiguranje cjelovitosti i sljedivosti svih informacijskih sustava, pri čemu je točnost vremena temeljni preduvjet.

10.2 P5 – Politika upravljanja promjenama. Uređuje izmjene konfiguracija sustava, uključujući prilagodbe izvora vremena, te osigurava odgovarajuću dokumentaciju, testiranje i planove povrata.

10.3 P22 – Politika bilježenja i nadzora. Izravno ovisi o sinkroniziranom vremenu radi osiguravanja redoslijeda događaja, korelacije dnevničkih zapisa i cjelovitosti istrage incidenta u različitim sustavima.

10.4 P30 – Politika odgovora na incidente. Oslanja se na točne vremenske oznake za forenzičke istrage, vremenski slijed incidenta i dokaze iz lanca nadzora. Netočno vrijeme narušava vjerodostojnost izvješća o incidentu.

10.5 P20 – Politika zaštite krajnjih uređaja / Politika zaštite od zlonamjernog softvera. Zahtijeva pravodobno upozoravanje i bihevioralnu analizu uz točne vremenske oznake radi otkrivanja širenja zlonamjernog softvera, bočnog kretanja i anomalija pristupa.

10.6 P6 – Politika upravljanja rizicima. Definira desinkronizaciju kao mogući operativni i forenzički rizik te zahtijeva kontrole definirane ovom politikom radi ublažavanja utjecaja.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – Operativno planiranje i kontrola: zahtijeva integraciju točnih tehničkih kontrola, kao što su sinkronizirani sustavni satovi, radi pouzdanog operativnog izvršavanja.

11.2 ISO/IEC 27002:2022 – Kontrola 8

11.2.1 Naglašava točnost sustavnog vremena i zahtijeva organizacijsku dosljednost vremena u sustavima radi usporedbe dnevničkih zapisa, istraga i sigurne provjere transakcija.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Sinkronizacija sustavnog vremena: zahtijeva sinkronizaciju vremena uporabom mjerodavnih izvora u svim komponentama unutar granice sustava.

11.3.2 AU-8 – Vremenske oznake: osigurava da događaji budu točno vremenski označeni i omogućuje sljedivost za reviziju i odgovor na incidente.

11.4 GDPR EU (2016/679)

11.4.1 Članak 32 – Sigurnost obrade: iako izričito ne navodi vrijeme, zahtijeva primjenu odgovarajućih tehničkih mjera — uključujući revizijske tragove i dnevničke zapise — koje za valjanost i cjelovitost inherentno ovise o sinkroniziranim vremenskim oznakama.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(e): zahtijeva mogućnosti bilježenja i otkrivanja koje pretpostavljaju točnu sinkronizaciju vremena radi korelacije među sustavima i pravodobnog odgovora.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – Upravljanje IKT rizicima: zahtijeva točnu sustavnu telemetriju za praćenje rizika i otkrivanje anomalija, što ovisi o preciznoj sinkronizaciji satova.

11.6.2 Članak 10 – Kontinuitet poslovanja IKT-a: nameće kontrole koje osiguravaju cjelovitost sustava tijekom prekida, uključujući vremenski usklađene zapise događaja.

11.7 COBIT 2019

11.7.1 DSS05.04 – Praćenje sigurnosnih događaja: zahtijeva cjelovitost vremenskih oznaka za učinkovitu analizu dnevničkih zapisa i otkrivanje prijetnji.

11.7.2 MEA03 – Praćenje, vrednovanje i procjena usklađenosti: sinkronizacija vremena podupire točne cikluse revizije usklađenosti i izvješćivanja.