					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P23					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	-
ISO/IEC 27002:2022	Kontrola 8	-
NIST SP 800-53 Rev. 5	SC-45, AU-8	-
Uredba EU GDPR	Člen 32	-
Direktiva EU NIS2	Člen 21(2)(e)	-
Uredba EU DORA	Člena 9, 10	-
COBIT 2019	DSS05.04, MEA03	-

1. Namen

1.1 Namen te politike je zagotoviti, da vsi sistemi, aplikacije, naprave in storitve v oblaku v organizaciji ohranjajo usklajene in točne časovne nastavitve s sinhronizacijo z določenimi zaupanja vrednimi časovnimi viri.

1.2 Natančna sinhronizacija časa je bistvena za zanesljivo beleženje dogodkov, revizijsko sled, varne komunikacije, odzivanje na incidente in forenzične preiskave. Neusklajen čas lahko povzroči neskladje v dnevnikih, neuspešno avtentikacijo in nepopolno poročanje regulatorju.

1.3 Ta politika podpira kontrolo 8.17 Priloge A standarda ISO/IEC 27001 in povezane mednarodne standarde, saj zahteva točnost časa in zaznavanje odstopanja sistemske ure v celotnem informacijskem okolju organizacije.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 vse komponente infrastrukture, vključno s strežniki, delovnimi postajami, omrežnimi napravami, požarnimi zidovi in sistemi interneta stvari (IoT)

2.1.2 virtualna okolja in okolja v oblaku (npr. AWS, Azure, Google Cloud)

2.1.3 vse sisteme, ki sodelujejo pri beleženju dnevnikov, avtentikaciji, obdelavi transakcij ali korelaciji varnostnih dogodkov

2.1.4 vse zaposlene, pogodbene izvajalce in ponudnike storitev tretjih oseb, ki so odgovorni za časovno občutljive sisteme

2.2 V področje uporabe spadajo tudi vsi sistemi, ki ustvarjajo ali uporabljajo časovno označene zapise, kot so vnosi v dnevnike, opozorila, evidence dejavnosti uporabnikov ali forenzični dokazi.

3. Cilji

3.1 Določiti dosledno in centralizirano arhitekturo sinhronizacije časa z uporabo odobrenih virov NTP ali enakovrednih rešitev.

3.2 Zagotoviti, da vsi sistemi sinhronizirajo sistemske ure v določenih intervalih ter da se vsako odstopanje zazna in odpravi samodejno ali z minimalnim posegom.

3.3 Ohraniti točnost sistemskih ur v hibridnih okoljih, lokalnih infrastrukturah in okoljih v oblaku, da se omogoči:

3.3.1 zanesljiva korelacija dogodkov in odzivanje na incidente

3.3.2 skladnost s standardi in predpisi, kot so ISO 27001, GDPR, NIS2 in DORA

3.3.3 zaščita pred ponovitvenimi napadi in napakami avtentikacije, povezanimi s časom

3.4 Vzpostaviti jasne vloge, postopke za obravnavo izjem in revizijske mehanizme za zagotavljanje izvajanja te politike.

3.5 Zagotoviti, da se anomalije, povezane s časom, beležijo v dnevnikih, sprožajo opozorila in izvajajo eskalacije, kadar presežejo določene tolerance.

4. Vloge in odgovornosti

4.1 vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost z operativnimi kontrolami sistema upravljanja informacijske varnosti (ISMS) in regulativnimi zahtevami.

4.1.2 Odobri izbiro časovnih virov na ravni organizacije in potrdi postopke poročanja o sinhronizaciji časa.

4.2 vodja infrastrukturnih storitev / vodja omrežnega inženiringa

4.2.1 Vzdržuje primarne in sekundarne strežnike NTP organizacije oziroma konfiguracijo določenih časovnih virov.

4.2.2 Zagotavlja, da vse omrežno povezane naprave in virtualne instance sinhronizirajo čas v ustreznih intervalih.

4.2.3 Spremlja dnevnike sinhronizacije časa, opozorila o odstopanju sistemske ure in stanja napak.

[... 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 To politiko je treba pregledati letno ali prej v naslednjih primerih:

9.1.1 zaznava izkoriščanja, povezanega s časom, ali odpovedi beleženja dnevnikov

9.1.2 spremembe v ključni časovni infrastrukturi (npr. novi strežniki NTP organizacije ali posodobitve protokolov)

9.1.3 neskladja pri odstopanju časa na oblačni platformi ali regionalne spremembe storitev

9.1.4 ugotovitve po incidentu, ki prepoznajo časovno neusklajenost kot prispevni dejavnik

9.2 Pregled koordinira vodja infrastrukture, pri čemer morajo sodelovati SOC, varnost aplikacij in predstavniki za skladnost.

9.3 Revizije morajo biti dokumentirane v registru dokumentov ISMS in sporočene prizadetim notranjim deležnikom ter deležnikom tretjih oseb.

9.4 Zgodovinske različice politike morajo biti varno arhivirane, verzionirane in na voljo za zahteve presoje skladnosti ali pravne revizije.

10. Povezane politike in povezave

10.1 P1 – Politika informacijske varnosti. Določa krovno zahtevo za zagotavljanje celovitosti in sledljivosti vseh informacijskih sistemov, pri čemer je točnost časa temeljnega pomena.

10.2 P5 – Politika upravljanja sprememb. Ureja spremembe sistemskih konfiguracij, vključno s prilagoditvami časovnih virov, ter zagotavlja ustrezno dokumentiranje, testiranje in načrte povrnitve.

10.3 P22 – Politika beleženja in spremljanja. Neposredno je odvisna od sinhroniziranega časa za zagotavljanje zaporedja dogodkov, korelacije dnevnikov in celovitosti preiskovanja incidentov v različnih sistemih.

10.4 P30 – Politika odzivanja na incidente. Zanaša se na natančne časovne žige za forenzične preiskave, časovnice incidentov in dokaze verige skrbništva. Netočen čas zmanjšuje verodostojnost poročil o incidentih.

10.5 P20 – Politika zaščite končnih točk / Politika zaščite pred zlonamerno programsko opremo. Zahteva časovno točna opozorila in analizo vedenja za zaznavanje širjenja zlonamerne programske opreme, lateralnega gibanja in anomalij dostopa.

10.6 P6 – Politika upravljanja tveganj. Opredeljuje desinhronizacijo kot potencialno operativno in forenzično tveganje ter zahteva kontrole iz te politike za zmanjšanje vpliva.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Operativno načrtovanje in nadzor: zahteva vključitev natančnih tehničnih kontrol, kot so sinhronizirane sistemske ure, za zanesljivo operativno izvajanje.

11.2 ISO/IEC 27002:2022 – Kontrola 8

11.2.1 Krepi zahtevo po točnosti sistemskih ur in doslednosti organizacijskega časa v sistemih, da se omogočijo primerjava dnevnikov, preiskovanje in varno potrjevanje transakcij.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-45 – Sinhronizacija sistemskega časa: zahteva sinhronizacijo časa z uporabo avtoritativnih virov v vseh komponentah znotraj meje sistema.

11.3.2 AU-8 – Časovni žigi: zagotavlja, da so dogodki natančno časovno označeni ter omogoča sledljivost za revizijo in odzivanje na incidente.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 32 – Varnost obdelave: čeprav časa ne navaja izrecno, zahteva uporabo ustreznih tehničnih ukrepov, vključno z revizijskimi sledmi in dnevniki, ki so za veljavnost in celovitost neločljivo odvisni od sinhroniziranih časovnih žigov.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(e): zahteva zmožnosti beleženja in zaznavanja, ki predpostavljajo natančno sinhronizacijo časa za korelacijo med sistemi in pravočasen odziv.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – upravljanje tveganj IKT: zahteva natančne sistemske telemetrične podatke za spremljanje tveganj in zaznavanje anomalij, kar je odvisno od natančne sinhronizacije sistemskih ur.

11.6.2 Člen 10 – neprekinjeno poslovanje IKT: zahteva kontrole, ki zagotavljajo celovitost sistema med motnjami, vključno s časovno usklajenimi evidencami dogodkov.

11.7 COBIT 2019

11.7.1 DSS05.04 – spremljanje varnostnih dogodkov: zahteva celovitost časovnih žigov za učinkovito analizo dnevnikov in zaznavanje groženj.

11.7.2 MEA03 – spremljanje, vrednotenje in presoja skladnosti: sinhronizacija časa podpira natančno presojo skladnosti in cikle poročanja.