					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P23S					Dokumenta nosaukums: **Laika sinhronizācijas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Attiecīgo kontroles pasākumu prasības
ISO/IEC 27002:2022	8. kontrole	Sinhronizēta sistēmu darbība
NIST SP 800-53 Rev.5	SC-45, AU-8	Uzticami NTP avoti un precīzi žurnālu laikspiedoli
ES GDPR	5. panta 1. punkta d) apakšpunkts, 32. pants	Personas datu precizitāte, pārskatatbildība un integritāte, ko nodrošina sinhronizēti laikspiedoli
ES NIS2	21. panta 2. punkta d) apakšpunkts	Uzraudzības un anomāliju noteikšanas spējas, ko nodrošina sinhronizēti žurnāli
ES DORA	10. pants, 15. pants	Operacionālā noturība un precīzi tehniskie ieraksti
COBIT 2019	DSS05.02, MEA03	Notikumu laikspiedoli un uz pierādījumiem balstīta uzraudzība

1. Mērķis

1.1 Šī politika nosaka obligātos kontroles pasākumus precīza un sinhronizēta laika uzturēšanai visās sistēmās, kas glabā, pārsūta vai apstrādā organizācijas datus.

1.2 Laika sinhronizācija ir būtiska, lai nodrošinātu sistēmu žurnālu izsekojamību, korektu drošības incidentu korelāciju un pierādījumu ticamību datorforensiskās analīzes vai juridiskas izvērtēšanas laikā.

1.3 Organizācijai jānodrošina automatizēta laika sinhronizācija kā pamatprasība audita integritātei, incidentu apstrādei un atbilstībai ISO 27001, GDPR, DORA un NIS2 prasībām.

1.4 Šī politika nodrošina, ka visas sistēmas izmanto uzticamus laika avotus, nepieļauj manuālu laika iestatījumu ignorēšanu un nosaka pienākumu savlaicīgi novērst sistēmas pulksteņa novirzes.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām uzņēmumam piederošām sistēmām un ierīcēm, tostarp serveriem, galddatoriem, klēpjdatoriem, mobilajām ierīcēm, ugunsmūriem, maršrutētājiem un virtuālajām mašīnām;

2.1.2 attālinātu un mākoņvidē izvietotu infrastruktūru, ko izmanto darbības nodrošināšanai (piemēram, AWS, Microsoft 365, SaaS platformas);

2.1.3 sistēmām, kas ģenerē vai glabā notikumu žurnālus, autentifikācijas ierakstus vai audita pēdas;

2.1.4 visiem darbiniekiem, līgumslēdzējiem, piegādātājiem vai ārējiem IT pakalpojumu sniedzējiem, kas ir atbildīgi par šo sistēmu konfigurēšanu vai uzturēšanu.

2.2 Politika attiecas arī uz BYOD galiekārtām, ko izmanto piekļuvei biznesa sistēmām, ja šīs galiekārtas glabā vai ģenerē auditam nozīmīgus datus.

3. Mērķi

3.1 Nodrošināt, ka visas kritiski svarīgās sistēmas automātiski sinhronizē laiku, izmantojot uzticamus Network Time Protocol (NTP) serverus vai līdzvērtīgus mākoņpakalpojumu sniedzēju mehānismus.

3.2 Novērst laika neatbilstības, kas var mazināt sistēmu žurnālu uzticamību vai korelācijas iespējas auditu vai drošības izmeklēšanu laikā.

3.3 Nodrošināt savlaicīgu laika noviržu noteikšanu un novēršanu, ja tās pārsniedz pieļaujamos sliekšņus.

3.4 Uzturēt konsekventu laikspiedolu piešķiršanu visās vidēs (lokālajā infrastruktūrā, mākoņvidē un attālinātajā vidē).

3.5 Izpildīt tehniskās un tiesiskās prasības attiecībā uz ierakstu un notikumu integritāti, izsekojamību un nenoliedzamību.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 apstiprina šo politiku un nodrošina tās ievērošanu visā organizācijā;

4.1.2 pārrauga periodisku sistēmu līmeņa laika precizitātes pārskatīšanu un ieviešanas nepilnību izvērtēšanu;

4.1.3 apstiprina izņēmumus no automatizētās laika sinhronizācijas, ja tie ir pamatoti un dokumentēti.

4.2 Ārējais IT pakalpojumu sniedzējs / iekšējā IT funkcija

4.2.1 konfigurē laika sinhronizāciju visām uzņēmumam piederošām vai pārvaldītām sistēmām;

4.2.2 pārbauda, vai ikdienas vai plānotā sinhronizācija darbojas pareizi;

4.2.3 izmeklē un novērš laika noviržu gadījumus, sinhronizācijas kļūmes vai NTP piekļuves problēmas;

4.2.4 dokumentē laika sinhronizācijas statusu ikmēneša sistēmu darbspējas pārbaužu ietvaros.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Plānotā pārskatīšana

9.1.1 Šī politika reizi gadā jāpārskata ģenerāldirektoram, ārējam IT pakalpojumu sniedzējam un privātuma koordinatoram.

9.1.2 Pārskatīšanā jāņem vērā visi žurnāli un pārskati par atbilstības statusu laika sinhronizācijas prasībām.

9.2 Uz ierosinātājiem balstīti atjauninājumi

9.2.1 Šī politika jāatjaunina, ja:

9.2.1.1 sistēmas kļūmes rezultātā rodas būtiska laika novirze;

9.2.1.2 audits atklāj nepilnības laika sinhronizācijā;

9.2.1.3 organizācija ievieš jaunas mākoņvides, hibrīdvides vai virtualizācijas vides;

9.2.1.4 tiesiskās vai regulatīvās izmaiņas nosaka jaunas prasības laika integritātei.

9.3 Versiju kontrole un komunikācija

9.3.1 Visi atjauninājumi jāversē un jādato.

9.3.2 Būtiskas izmaiņas jāpaziņo visam tehniskajam personālam.

9.3.3 Iepriekšējās versijas jāglabā 3 gadus audita vajadzībām.

10. Saistītās politikas un sasaiste

10.1 Šī politika jāpiemēro kopā ar šādām SME politikām:

10.1.1 P22S – Žurnālfiksēšanas un uzraudzības politika: nodrošina konsekventu laikspiedolu piešķiršanu žurnālos izsekojamībai un datorforensiskajai korelācijai.

10.1.2 P30S – Incidentu reaģēšanas politika: balstās uz precīziem laikspiedoliem, lai rekonstruētu incidentus, noteiktu laika līnijas un pamatotu paziņošanas lēmumus.

10.1.3 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka piekļuves žurnāli un datu apstrādes termiņi, kas saistīti ar personas datiem, ir precīzi un aizstāvami atbilstoši GDPR.

10.1.4 P12S – Aktīvu pārvaldības politika: atbalsta to sistēmu identificēšanu, kurām nepieciešama sinhronizācija, jo īpaši mobilajām un attālinātajām ierīcēm.

10.1.5 P26S – Trešo pušu un piegādātāju drošības politika: nodrošina, ka piegādātāji, kuri organizācijas vārdā piekļūst datiem vai ģenerē to žurnālus, līgumiski ievēro sinhronizēta laika prasības.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 8. punkts – nosaka prasību ieviest drošai darbībai nepieciešamos kontroles pasākumus, tostarp žurnālfiksēšanu un laikspiedolu izmantošanu.

11.2 ISO/IEC 27002:

11.2.1 8.17. kontrole – iesaka sinhronizētu laiku visām sistēmām, kas ģenerē žurnālus vai darbojas savstarpēji saistīti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – nosaka prasību izmantot iekšējus vai ārējus laika avotus žurnālu laikspiedolu precizitātes nodrošināšanai.

11.3.2 SC-45 – nosaka uzticamu NTP avotu izmantošanu un manuālu laika izmaiņu novēršanu kritiski svarīgās sistēmās.

11.4 ES GDPR:

11.4.1 5. panta 1. punkta d) apakšpunkts – nosaka precizitātes un pārskatatbildības prasību personas datu apstrādē, ko atbalsta sinhronizēti laikspiedoli.

11.4.2 32. pants – nosaka drošības pasākumus datu integritātes nodrošināšanai, tostarp konsekventus žurnālfiksēšanas laika ietvarus.

11.5 ES NIS2 direktīva:

11.5.1 21. panta 2. punkta d) apakšpunkts – nosaka uzraudzības un noteikšanas spēju prasību, ko atbalsta sinhronizēti sistēmu žurnāli.

11.6 ES DORA:

11.6.1 10. pants – nosaka operacionālās noturības prasību, kas paredz izsekojamus IKT incidentu žurnālus ar laikspiedoliem.

11.6.2 15. pants – nosaka prasību pakalpojumu sniedzējiem uzturēt precīzus tehniskos ierakstus, tostarp audita pēdas ar laikspiedoliem.

11.7 COBIT 2019:

11.7.1 DSS05.02 – uzsver laikspiedolu integritātes nozīmi notikumu noteikšanā un reaģēšanā uz tiem.

11.7.2 MEA03.01 – nosaka uz pierādījumiem balstītu veiktspējas uzraudzību, ko atbalsta precīzi un laikā sinhronizēti dati.