					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P23					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	-
ISO/IEC 27002:2022	8. kontrole	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
ES GDPR	32. pants	-
ES NIS2	21. panta 2. punkta e) apakšpunkts	-
ES DORA	9., 10. pants	-
COBIT 2019	DSS05.04, MEA	-

1. Mērķis

1.1 Šīs politikas mērķis ir nodrošināt, ka visas organizācijas sistēmas, lietojumprogrammas, ierīces un mākoņpakalpojumi uztur vienotus un precīzus laika iestatījumus, sinhronizējoties ar norādītiem un uzticamiem laika avotiem.

1.2 Precīza laika sinhronizācija ir būtiska uzticamai žurnalēšanai, drošai saziņai, audita izsekojamībai, incidentu pārvaldībai un digitālajai kriminālistikai. Nesinhronizēts laiks var radīt nesavietojamus žurnālus, autentifikācijas kļūmes un nepilnīgu normatīvo prasību izpildi attiecībā uz ziņošanu.

1.3 Šī politika atbalsta ISO/IEC 27001 A pielikuma 8.17. kontroli un saistītos starptautiskos standartus, nodrošinot laika precizitāti un sistēmu pulksteņu noviržu noteikšanu visā organizācijas IT vidē.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām infrastruktūras komponentēm, tostarp serveriem, darbstacijām, tīkla ierīcēm, ugunsmūriem un IoT sistēmām;

2.1.2 virtuālajām un mākoņvidēm (piemēram, AWS, Azure, Google Cloud);

2.1.3 visām sistēmām, kas piedalās žurnalēšanā, autentifikācijā, darījumu apstrādē vai drošības notikumu korelācijā;

2.1.4 iekšējiem darbiniekiem, līgumdarbiniekiem un trešo pušu pakalpojumu sniedzējiem, kuri ir atbildīgi par laika ziņā jutīgām sistēmām.

2.2 Sistēmas, kas ģenerē vai izmanto ierakstus ar laika zīmogiem, piemēram, žurnālierakstus, brīdinājumus, lietotāju darbību ierakstus vai digitālās kriminālistikas pierādījumus, ir uzskatāmas par ietvertām šīs politikas piemērošanas jomā.

3. Mērķi

3.1 Definēt vienotu, centralizētu laika sinhronizācijas arhitektūru, izmantojot apstiprinātus NTP avotus vai līdzvērtīgus risinājumus.

3.2 Nodrošināt, ka visas sistēmas sinhronizē savus pulksteņus noteiktos intervālos un ka jebkura novirze tiek noteikta un koriģēta automātiski vai ar minimālu iejaukšanos.

3.3 Uzturēt pulksteņu precizitāti hibrīdvidēs, lokāli izvietotā infrastruktūrā un mākoņvidēs, lai nodrošinātu:

3.3.1 uzticamu notikumu korelāciju un incidentu pārvaldību;

3.3.2 atbilstību tādiem standartiem kā ISO 27001, GDPR, NIS2 un DORA;

3.3.3 aizsardzību pret atkārtojuma uzbrukumiem un uz laiku balstītām autentifikācijas kļūmēm.

3.4 Noteikt skaidras lomas, izņēmumu pārvaldības procedūras un audita mehānismus, lai nodrošinātu politikas ievērošanu.

3.5 Nodrošināt, ka ar laiku saistītas anomālijas tiek reģistrētas žurnālos, par tām tiek ģenerēti brīdinājumi un tās tiek eskalētas, ja tiek pārsniegtas noteiktās pielaides.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 ir šīs politikas īpašnieks un nodrošina tās saskaņotību ar IDPS darbības kontroles pasākumiem un normatīvajām prasībām;

4.1.2 apstiprina uzņēmuma laika avotu izvēli un validē laika sinhronizācijas ziņošanas procesus.

4.2 Infrastruktūras pakalpojumu vadītājs / tīklu inženierijas vadītājs

4.2.1 uztur organizācijas primāro un sekundāro NTP serveru vai norādīto laika avotu konfigurāciju;

4.2.2 nodrošina, ka visas tīklam pievienotās ierīces un virtuālās instances sinhronizē laiku atbilstošos intervālos;

4.2.3 uzrauga laika sinhronizācijas žurnālus, pulksteņu noviržu brīdinājumus un kļūmju statusus.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata reizi gadā vai agrāk šādos gadījumos:

9.1.1 tiek konstatēti uz laiku balstīti izmantošanas paņēmieni vai žurnalēšanas kļūmes;

9.1.2 notiek izmaiņas pamatlaika infrastruktūrā (piemēram, jauni uzņēmuma NTP serveri vai protokolu atjauninājumi);

9.1.3 tiek konstatētas laika noviržu neatbilstības mākoņplatformās vai reģionālas pakalpojumu izmaiņas;

9.1.4 pēc incidenta konstatējumi identificē laika nesaskaņotību kā veicinošu faktoru.

9.2 Pārskatīšanu koordinē infrastruktūras vadītājs, piesaistot nepieciešamo ieguldījumu no SOC, lietojumprogrammu drošības un atbilstības iesaistītajām pusēm.

9.3 Grozījumi jādokumentē IDPS dokumentu reģistrā un jāpaziņo ietekmētajām iekšējām un trešo pušu iesaistītajām pusēm.

9.4 Politikas vēsturiskās versijas droši jāarhivē, jāpārvalda versiju kontrolē un jāpadara pieejamas atbilstības vai juridiskā audita pieprasījumiem.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Tā nosaka vispārējo prasību nodrošināt visu informācijas sistēmu integritāti un izsekojamību, kuras pamatā ir precīzs laiks.

10.2 P5 – Izmaiņu pārvaldības politika. Tā regulē izmaiņas sistēmu konfigurācijās, tostarp laika avotu pielāgojumus, nodrošinot pienācīgu dokumentēšanu, testēšanu un izmaiņu atcelšanas plānus.

10.3 P22 – Žurnalēšanas un uzraudzības politika. Tā tieši ir atkarīga no sinhronizēta laika, lai nodrošinātu notikumu secību, žurnālu korelāciju un incidentu izmeklēšanas integritāti dažādās sistēmās.

10.4 P30 – Incidentu reaģēšanas politika. Tā balstās uz precīziem laika zīmogiem digitālajā kriminālistikā, incidentu laika skalās un pierādījumu glabāšanas ķēdē. Neprecīzs laiks mazina incidentu ziņojumu ticamību.

10.5 P20 – Galapunktu aizsardzības / ļaunprogrammatūras politika. Tā prasa laika ziņā precīzu brīdināšanu un uzvedības analīzi, lai atklātu ļaunprogrammatūras izplatīšanos, sānu pārvietošanos un piekļuves anomālijas.

10.6 P6 – Risku pārvaldības politika. Tā definē desinhronizācijas apstrādi kā iespējamu darbības un digitāli kriminālistisko risku, kam ietekmes mazināšanai jāpiemēro šajā politikā noteiktie kontroles pasākumi.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8.1. punkts – darbības plānošana un kontrole: prasa integrēt precīzus tehniskos kontroles pasākumus, piemēram, sinhronizētus sistēmu pulksteņus, lai nodrošinātu uzticamu darbības izpildi.

11.2 ISO/IEC 27002:2022 – 8. kontrole

11.2.1 Tā nostiprina pulksteņu precizitātes prasību un nosaka organizatorisku sistēmas laika vienotību, lai atvieglotu žurnālu salīdzināšanu, izmeklēšanu un drošu darījumu validāciju.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-45 – sistēmas laika sinhronizācija: prasa laika sinhronizāciju, izmantojot autoritatīvus avotus visās komponentēs sistēmas robežās.

11.3.2 AU-8 – laika zīmogi: nodrošina, ka notikumiem tiek piešķirti precīzi laika zīmogi un nodrošināta izsekojamība auditam un incidentu pārvaldībai.

11.4 ES GDPR (2016/679)

11.4.1 32. pants – apstrādes drošība: lai gan tajā laiks nav minēts tieši, tas nosaka atbilstošu tehnisko pasākumu izmantošanu, tostarp audita pēdas un žurnālus, kuru derīgums un integritāte pēc būtības ir atkarīga no sinhronizētiem laika zīmogiem.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta e) apakšpunkts: prasa žurnalēšanas un atklāšanas spējas, kuru priekšnoteikums ir precīza laika sinhronizācija starpsistēmu korelācijai un savlaicīgai reaģēšanai.

11.6 ES DORA (2022/2554)

11.6.1 9. pants – IKT risku pārvaldība: nosaka prasību par precīzu sistēmu telemetriju riska uzraudzībai un anomāliju noteikšanai, kas ir atkarīga no precīzas pulksteņu sinhronizācijas.

11.6.2 10. pants – IKT darbības nepārtrauktība: nosaka kontroles pasākumus sistēmu integritātes nodrošināšanai traucējumu laikā, tostarp laika ziņā saskaņotus notikumu ierakstus.

11.7 COBIT 2019

11.7.1 DSS05.04 – drošības notikumu uzraudzība: prasa laika zīmogu integritāti efektīvai žurnālu analīzei un apdraudējumu noteikšanai.

11.7.2 MEA03 – atbilstības uzraudzība, izvērtēšana un novērtēšana: laika sinhronizācija atbalsta precīzus atbilstības auditus un ziņošanas ciklus.