					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P23					Asiakirjan nimi: **Aikasynkronointipolitiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja sääntelyvaatimusten kanssa

Standardi/sääntely	Kohta/artikla	Kommentti
ISO/IEC 27001:2022	Luku 8	-
ISO/IEC 27002:2022	Kontrolli 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
EU:n GDPR	Artikla 32	-
EU:n NIS2-direktiivi	Artikla 21(2)(e)	-
EU:n DORA-asetus	Artiklat 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Tarkoitus

1.1 Tämän politiikan tarkoituksena on varmistaa, että kaikki organisaation järjestelmät, sovellukset, laitteet ja pilvipalvelut ylläpitävät yhdenmukaisia ja tarkkoja aika-asetuksia synkronoimalla nimetettyihin, luotettuihin aikalähteisiin.

1.2 Tarkka aikasynkronointi on välttämätöntä luotettavan lokituksen, turvallisen viestinnän, auditointijäljen jäljitettävyyden, poikkeamien käsittelyn ja forensisten tutkimusten kannalta. Kellonaikojen epäsynkronia voi johtaa lokitietojen korreloimattomuuteen, todennuksen epäonnistumiseen ja puutteelliseen sääntelyraportointiin.

1.3 Tämä politiikka tukee ISO/IEC 27001:n liitteen A kontrollia 8.17 ja siihen liittyviä kansainvälisiä standardeja varmistamalla ajan tarkkuuden ja kellopoikkeamien havaitsemisen koko organisaation IT-ympäristössä.

2. Soveltamisala

2.1 Tämä politiikka koskee seuraavia:

2.1.1 kaikki infrastruktuurikomponentit, mukaan lukien palvelimet, työasemat, verkkolaitteet, palomuurit ja IoT-järjestelmät

2.1.2 virtuaali- ja pilviympäristöt (esim. AWS, Azure, Google Cloud)

2.1.3 kaikki järjestelmät, jotka osallistuvat lokitukseen, todennukseen, tapahtumien käsittelyyn tai tietoturvatapahtumien korrelointiin

2.1.4 organisaation työntekijät, urakoitsijat ja kolmannen osapuolen palveluntarjoajat, joilla on vastuu aikaherkistä järjestelmistä

2.2 Järjestelmät, jotka tuottavat tai käyttävät aikaleimattuja tietueita, kuten lokimerkintöjä, hälytyksiä, käyttäjätoiminnan tallenteita tai forensista todistusaineistoa, kuuluvat tämän politiikan soveltamisalaan.

3. Tavoitteet

3.1 Määrittää yhdenmukainen, keskitetty aikasynkronoinnin arkkitehtuuri käyttäen hyväksyttyjä NTP-lähteitä tai vastaavia ratkaisuja.

3.2 Varmistaa, että kaikki järjestelmät synkronoivat kellonsa määritellyin aikavälein ja että mahdollinen poikkeama havaitaan ja korjataan automaattisesti tai vähäisellä manuaalisella toimenpiteellä.

3.3 Ylläpitää kellon tarkkuutta hybridiympäristöissä, omissa tiloissa ja pilviympäristöissä, jotta voidaan mahdollistaa:

3.3.1 luotettava tapahtumien korrelointi ja poikkeamien käsittely

3.3.2 vaatimustenmukaisuus standardien, kuten ISO 27001:n, GDPR:n, NIS2:n ja DORA:n, kanssa

3.3.3 suojaus toistohyökkäyksiltä ja aikaan perustuvilta todennuksen epäonnistumisilta

3.4 Määrittää selkeät roolit, poikkeustenhallintamenettelyt ja auditointimekanismit politiikan soveltamisen ylläpitämiseksi.

3.5 Varmistaa, että aikaan liittyvät poikkeamat kirjataan lokiin, niistä muodostetaan hälytys ja ne eskaloidaan, kun ne ylittävät sallitut rajat.

4. Roolit ja vastuut

4.1 Tietoturvajohtaja (CISO)

4.1.1 Omistaa tämän politiikan ja varmistaa sen yhdenmukaisuuden tietoturvallisuuden hallintajärjestelmän (ISMS), operatiivisten kontrollien ja sääntelyvaatimusten kanssa.

4.1.2 Hyväksyy organisaation aikalähteiden valinnan ja validoi aikasynkronoinnin raportointiprosessit.

4.2 Infrastruktuuripalveluista vastaava päällikkö / verkkotekniikan vastuuhenkilö

4.2.1 Ylläpitää organisaation ensisijaisia ja toissijaisia NTP-palvelimia tai nimettyä aikalähdemääritystä.

4.2.2 Varmistaa, että kaikki verkkoon liitetyt laitteet ja virtuaali-instanssit synkronoivat ajan määritellyin aikavälein.

4.2.3 Seuraa aikasynkronoinnin lokeja, kellopoikkeamahälytyksiä ja vikatilanteita.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vuosittain tai aiemmin seuraavissa tilanteissa:

9.1.1 aikaan perustuvien hyväksikäyttömenetelmien tai lokituksen epäonnistumisten havaitseminen

9.1.2 muutokset keskeisessä aikainfrastruktuurissa (esim. uudet organisaation NTP-palvelimet tai protokollapäivitykset)

9.1.3 pilvialustojen kellopoikkeamiin liittyvät ristiriidat tai alueelliset palvelumuutokset

9.1.4 poikkeaman jälkiarvioinnin havainnot, joissa ajan epäsynkronia on tunnistettu myötävaikuttavaksi tekijäksi

9.2 Katselmoinnin koordinoinnista vastaa infrastruktuurivastaava, ja siihen on saatava tarvittava osallistuminen tietoturvavalvomolta (SOC), sovellustietoturvalta ja vaatimustenmukaisuuden sidosryhmiltä.

9.3 Muutokset on dokumentoitava ISMS:n asiakirjahallintarekisteriin ja viestittävä vaikutuksen alaisille sisäisille ja kolmannen osapuolen sidosryhmille.

9.4 Politiikan historialliset versiot on arkistoitava turvallisesti, pidettävä versionhallittuina ja asetettava saataville vaatimustenmukaisuutta tai oikeudellisia auditointipyyntöjä varten.

10. Liittyvät politiikat ja yhteydet

10.1 P1 – Tietoturvapolitiikka. Määrittää yleisen velvoitteen varmistaa kaikkien tietojärjestelmien eheys ja jäljitettävyys, joiden perustana ajan tarkkuus toimii.

10.2 P5 – Muutoksenhallintapolitiikka. Ohjaa järjestelmämääritysten muutoksia, mukaan lukien aikalähteiden muutokset, varmistaen asianmukaisen dokumentoinnin, testauksen ja palautussuunnitelmat.

10.3 P22 – Lokitus- ja valvontapolitiikka. Riippuu suoraan synkronoidusta ajasta tapahtumien järjestyksen, lokien korrelaation ja poikkeamatutkinnan eheyden varmistamiseksi eri järjestelmissä.

10.4 P30 – Tietoturvapoikkeamien hallintapolitiikka. Tukeutuu tarkkoihin aikaleimoihin forensisia tutkimuksia, poikkeamien aikajanoja ja hallussapitoketjun todistusaineistoa varten. Epätarkka aika heikentää poikkeamaraporttien luotettavuutta.

10.5 P20 – Päätelaitesuojaus / haittaohjelmapolitiikka. Edellyttää ajallisesti tarkkaa hälytystä ja käyttäytymisanalyysiä haittaohjelmien leviämisen, lateraalisen liikkumisen ja käyttöpoikkeamien havaitsemiseksi.

10.6 P6 – Riskienhallintapolitiikka. Määrittää epäsynkronoinnin käsittelyn mahdollisena operatiivisena ja forensisena riskinä ja edellyttää tässä politiikassa määriteltyjä kontrolleja vaikutusten lieventämiseksi.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Luku 8.1 – Operatiivinen suunnittelu ja ohjaus: edellyttää tarkkojen teknisten kontrollien, kuten synkronoitujen järjestelmäkellojen, integrointia luotettavaa operatiivista toteutusta varten.

11.2 ISO/IEC 27002:2022 – Kontrolli 8

11.2.1 Korostaa kellon tarkkuuden merkitystä ja edellyttää organisaation järjestelmäajan yhdenmukaisuutta lokien vertailun, tutkinnan ja turvallisen tapahtumavalidoinnin mahdollistamiseksi.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Järjestelmäajan synkronointi: edellyttää aikasynkronointia käyttäen ajantasaisia lähteitä kaikissa järjestelmän rajauksen sisäisissä komponenteissa.

11.3.2 AU-8 – Aikaleimat: varmistaa, että tapahtumat aikaleimataan tarkasti ja että auditointia ja tietoturvapoikkeamiin reagointia varten on jäljitettävyys.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 32 – käsittelyn turvallisuus: vaikka artiklassa ei nimenomaisesti viitata aikaan, se edellyttää asianmukaisia teknisiä toimenpiteitä, mukaan lukien auditointijäljet ja lokit, joiden pätevyys ja eheys ovat luontaisesti riippuvaisia synkronoiduista aikaleimoista.

11.5 EU:n NIS2-direktiivi (2022/2555)

11.5.1 Artikla 21(2)(e): edellyttää lokitusta ja havaitsemiskyvykkyyksiä, jotka perustuvat tarkkaan aikasynkronointiin järjestelmien välisen korrelaation ja oikea-aikaisen reagoinnin mahdollistamiseksi.

11.6 EU:n DORA-asetus (2022/2554)

11.6.1 Artikla 9 – ICT-riskien hallinta: edellyttää tarkkaa järjestelmätelemetriaa riskien seurannan ja poikkeamien havaitsemisen tueksi, mikä riippuu täsmällisestä kellon synkronoinnista.

11.6.2 Artikla 10 – ICT-liiketoiminnan jatkuvuus: edellyttää kontrolleja, joilla varmistetaan järjestelmien eheys häiriöiden aikana, mukaan lukien ajallisesti yhdenmukaiset tapahtumatallenteet.

11.7 COBIT 2019

11.7.1 DSS05.04 – Tietoturvatapahtumien seuranta: edellyttää aikaleimojen eheyttä tehokasta lokianalyysia ja uhkien havaitsemista varten.

11.7.2 MEA03 – Vaatimustenmukaisuuden seuranta, arviointi ja tarkastelu: aikasynkronointi tukee tarkkaa vaatimustenmukaisuuden auditointia ja raportointisyklejä.