					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P23S					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	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 8	Asiaankuuluvat kontrollivaatimukset
ISO/IEC 27002:2022	Kontrolli 8	Synkronoitu järjestelmätoiminta
NIST SP 800-53 Rev.5	SC-45, AU-8	Luotettu NTP ja lokien aikaleimojen tarkkuus
EU:n GDPR	Artiklat 5(1)(d), 32	Henkilötietojen tarkkuus, osoitusvelvollisuus ja eheys synkronoitujen aikaleimojen avulla
EU:n NIS2-direktiivi	Artikla 21(2)(d)	Seuranta- ja havaitsemiskyvykkyydet, joita synkronoidut lokit tukevat
EU:n DORA-asetus	Artiklat 10, 15	Operatiivinen häiriönsietokyky ja tarkat tekniset tallenteet
COBIT 2019	DSS05.02, MEA03	Aikaleimatut tapahtumat ja näyttöön perustuva seuranta

1. Tarkoitus

1.1 Tällä politiikalla määritetään pakolliset kontrollit tarkan ja synkronoidun ajan ylläpitämiseksi kaikissa järjestelmissä, jotka tallentavat, siirtävät tai käsittelevät organisaation tietoja.

1.2 Aikasynkronointi on olennainen edellytys sille, että järjestelmälokit ovat jäljitettävissä, tietoturvapoikkeamat voidaan korreloida tarkasti ja todistusaineistoon voidaan luottaa forensisessa analyysissä tai oikeudellisessa tarkastelussa.

1.3 Organisaatio edellyttää automatisoitua aikasynkronointia perustavanlaatuisena vaatimuksena auditointien eheyden, tietoturvapoikkeamiin reagoinnin ja ISO 27001:n, EU:n GDPR:n, DORA-asetuksen ja EU:n NIS2-direktiivin mukaisten vaatimustenmukaisuusvelvoitteiden täyttämiseksi.

1.4 Tällä politiikalla varmistetaan, että kaikki järjestelmät käyttävät luotettuja aikalähteitä, ajan asetusten manuaaliset ohitukset estetään ja kellon poikkeamat korjataan viivytyksettä.

2. Soveltamisala

2.1 Tämä politiikka koskee seuraavia:

2.1.1 Kaikkia yrityksen omistamia järjestelmiä ja laitteita, mukaan lukien palvelimet, pöytätietokoneet, kannettavat tietokoneet, mobiililaitteet, palomuurit, reitittimet ja virtuaalikoneet

2.1.2 Etä- ja pilvi-infrastruktuuria, jota käytetään operatiivisessa toiminnassa (esim. AWS, Microsoft 365, SaaS-ympäristöt)

2.1.3 Järjestelmiä, jotka tuottavat tai tallentavat tapahtumalokeja, todennustietoja tai auditointijälkiä

2.1.4 Jokaista työntekijää, toimeksisaajaa, toimittajaa tai IT-tukipalveluntarjoajaa, joka vastaa näiden järjestelmien konfiguroinnista tai ylläpidosta

2.2 Tätä politiikkaa sovelletaan myös BYOD-päätelaitteisiin, joita käytetään yrityksen järjestelmien käyttöön, jos kyseiset päätelaitteet tallentavat tai tuottavat auditoinnin kannalta merkityksellisiä tietoja.

3. Tavoitteet

3.1 Varmistaa, että kaikki kriittiset järjestelmät synkronoivat ajan automaattisesti luotettujen NTP-palvelinten tai vastaavien pilvipalveluntarjoajan mekanismien avulla

3.2 Estää aikaerot, jotka voisivat heikentää järjestelmälokien luotettavuutta tai korreloitavuutta auditoinneissa tai tietoturvatutkinnoissa

3.3 Mahdollistaa hyväksyttävät raja-arvot ylittävien kellopoikkeamien oikea-aikaisen havaitsemisen ja korjaamisen

3.4 Ylläpitää yhdenmukainen aikaleimaus kaikissa ympäristöissä (omissa tiloissa, pilviympäristöissä ja etäympäristöissä)

3.5 Täyttää tallenteiden ja tapahtumien eheyteen, jäljitettävyyteen ja kiistämättömyyteen liittyvät tekniset ja oikeudelliset vaatimukset

4. Roolit ja vastuut

4.1 Toimitusjohtaja (GM)

4.1.1 Hyväksyy tämän politiikan ja varmistaa organisaation vaatimustenmukaisuuden

4.1.2 Valvoo järjestelmätason ajan tarkkuuden ja toteutuksen puutteiden säännöllisiä katselmointeja

4.1.3 Hyväksyy poikkeukset automatisoidusta aikasynkronoinnista, jos ne ovat perusteltuja ja dokumentoituja

4.2 IT-tukipalveluntarjoaja / sisäinen IT-vastaava

4.2.1 Konfiguroi aikasynkronoinnin kaikille yrityksen omistamille tai hallinnoimille järjestelmille

4.2.2 Varmistaa päivittäin tai sovitun aikataulun mukaisesti, että synkronointi toimii oikein

4.2.3 Tutkii ja korjaa kellopoikkeamat, synkronointivirheet tai NTP-yhteysongelmat

4.2.4 Dokumentoi aikasynkronoinnin tilan osana kuukausittaisia järjestelmien toimintakuntotarkastuksia

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Aikataulutettu katselmointi

9.1.1 Toimitusjohtajan, IT-tukipalveluntarjoajan ja tietosuojakoordinaattorin on katselmoitava tämä politiikka vuosittain

9.1.2 Katselmoinnissa on otettava huomioon kaikki lokit sekä aikasynkronoinnin vaatimustenmukaisuuden tilaraportit

9.2 Heräteperusteiset päivitykset

9.2.1 Tämä politiikka on päivitettävä, jos:

9.2.1.1 Järjestelmävika aiheuttaa merkittävän kellopoikkeaman

9.2.1.2 Auditointi paljastaa puutteita aikasynkronoinnissa

9.2.1.3 Organisaatio ottaa käyttöön uusia pilvi-, hybridi- tai virtualisointiympäristöjä

9.2.1.4 Lainsäädännön tai sääntelyn muutokset tuovat uusia ajan eheyteen liittyviä vaatimuksia

9.3 Versionhallinta ja viestintä

9.3.1 Kaikki päivitykset on versioitava ja päivättävä

9.3.2 Merkittävistä muutoksista on tiedotettava kaikelle tekniselle henkilöstölle

9.3.3 Aiemmat versiot on säilytettävä kolmen vuoden ajan auditoinnin tueksi

10. Liittyvät politiikat ja yhteydet

10.1 Tätä politiikkaa on sovellettava yhdessä seuraavien pk-yrityksen politiikkojen kanssa:

10.1.1 P22S – Lokitus- ja valvontapolitiikka: Varmistaa yhdenmukaisen aikaleimauksen kaikissa lokeissa jäljitettävyyden ja forensisen korrelaation tukemiseksi.

10.1.2 P30S – Tietoturvapoikkeamien hallintapolitiikka: Perustuu aikaleimojen tarkkuuteen poikkeamien rekonstruoimiseksi, aikajanojen määrittämiseksi ja ilmoituspäätösten tueksi.

10.1.3 P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Varmistaa, että henkilötietoihin liittyvät käyttölokit ja tietojen käsittelyn aikajanat ovat tarkkoja ja EU:n GDPR:n näkökulmasta perusteltavissa.

10.1.4 P12S – Omaisuudenhallintapolitiikka: Tukee niiden järjestelmien tunnistamista, jotka edellyttävät synkronointia, erityisesti mobiili- ja etälaitteiden osalta.

10.1.5 P26S – Kolmannen osapuolen ja toimittajaturvallisuuden politiikka: Varmistaa sopimuksellisesti, että toimittajat, jotka käyttävät organisaation tietoja tai tuottavat niistä lokitietoja, noudattavat synkronoidun ajan käytäntöjä.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001:

11.1.1 Lauseke 8.1 – Edellyttää turvallisten toimintojen kannalta tarpeellisten kontrollien toteuttamista, mukaan lukien lokitus ja aikaleimaus.

11.2 ISO/IEC 27002:

11.2.1 Kontrolli 8.17 – Suosittelee synkronoitua aikaa kaikille järjestelmille, jotka tuottavat lokeja tai toimivat yhteistoiminnallisesti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Edellyttää sisäisten tai ulkoisten aikalähteiden käyttöä lokien aikaleimojen tarkkuuden varmistamiseksi.

11.3.2 SC-45 – Määrittää luotettujen NTP-lähteiden käytön ja manuaalisten ajanmuutosten estämisen kriittisissä järjestelmissä.

11.4 EU:n GDPR:

11.4.1 Artikla 5(1)(d) – Edellyttää henkilötietojen käsittelyn tarkkuutta ja osoitusvelvollisuutta, joita synkronoidut aikaleimat tukevat.

11.4.2 Artikla 32 – Edellyttää tietojen eheyden varmistavia turvatoimia, joihin kuuluu johdonmukainen lokituksen aikakehys.

11.5 EU:n NIS2-direktiivi:

11.5.1 Artikla 21(2)(d) – Edellyttää seuranta- ja havaitsemiskyvykkyyksiä, joita synkronoidut järjestelmälokit tukevat.

11.6 EU:n DORA-asetus:

11.6.1 Artikla 10 – Edellyttää operatiivista häiriönsietokykyä, mikä vaatii jäljitettävät ja aikaleimatut ICT-poikkeamalokit.

11.6.2 Artikla 15 – Edellyttää palveluntarjoajilta tarkkojen teknisten tallenteiden ylläpitoa, mukaan lukien aikaleimatut auditointijäljet.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Korostaa aikaleimojen eheyttä tapahtumien havaitsemisessa ja niihin reagoinnissa.

11.7.2 MEA03.01 – Edellyttää näyttöön perustuvaa suorituskyvyn seurantaa, jota tarkat ja aikasynkronoidut tiedot tukevat.