					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P16S					Asiakirjan nimi: **Tietojen peittämistä ja pseudonymisointia koskeva politiikka**							
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	Kohta 6.1.3, kohta 8	Tietoturvariskit ja tarvittavat kontrollit, mukaan lukien peittäminen ja pseudonymisointi
ISO/IEC 27002:2022	Kontrollit 8.11, 8.12	Ohjeistus tietojen peittämisestä ja tietovuotojen estämisestä
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Tietojen hämärtäminen ja tietosuojaa parantavat teknologiat
EU:n NIS2-direktiivi	Artikla 21(2)(c)	Oikeasuhteiset tekniset toimenpiteet, pseudonymisointi kontrollina
EU:n DORA-asetus	Artikla 10(1)	ICT-riskien hallintakeinot, mukaan lukien tietojen muuntamiseen liittyvät suojatoimet
COBIT 2019	DSS05.01, DSS06	Tietosuoja sekä hämärtämis- ja pseudonymisointitekniikat
EU:n GDPR	Artiklat 4(5), 5(1)(c), 32	Tietojen minimointi ja pseudonymisointi teknisenä hallintakeinona

1. Tarkoitus

1.1. Tässä politiikassa määritellään velvoittavat vaatimukset tietojen peittämisen ja pseudonymisoinnin käytölle henkilötietojen, luottamuksellisten tietojen ja muiden arkaluonteisten tietojen suojaamiseksi pienissä ja keskisuurissa yrityksissä.

1.2. Näiden menetelmien käyttö on pakollista silloin, kun aitoja tietoja ei tarvita, kuten kehityksessä, analytiikassa tai kolmansien osapuolten palvelutilanteissa, jotta altistumisen, väärinkäytön tai tietoturvaloukkauksen riskiä vähennetään.

1.3. Tämä politiikka tukee suoraan ISO/IEC 27001:2022 -sertifioinnin vaatimuksia sekä eurooppalaisia sääntelyvelvoitteita, kuten EU:n GDPR:ää, EU:n NIS2-direktiiviä ja EU:n DORA-asetusta.

1.4. Muuntamalla tiedot ennen niiden käyttöä alkuperäisen liiketoimintayhteyden ulkopuolella organisaatio rajoittaa vastuualtistustaan ja parantaa valmiuttaan osoittaa tietosuojaan ja tietoturvaan liittyvää huolellisuutta.

2. Soveltamisala

2.1. Tämä politiikka koskee kaikkea rakenteista ja rakenteetonta tietoa, joka on luokiteltu henkilötiedoksi, luottamukselliseksi tai arkaluonteiseksi ja jota säilytetään tai käsitellään:

2.1.1. tuotanto-, testi- tai kehitysympäristöissä

2.1.2. paikallisilla laitteilla, palvelimilla tai pilvialustoilla

2.1.3. sisäisen henkilöstön, sopimuskumppaneiden tai kolmansien osapuolten palveluntarjoajien toimesta

2.2. Politiikka kattaa myös kaikki tietojen muuntamiseen käytettävät työkalut (peittäminen, tokenisointi, pseudonymisointi) riippumatta siitä, ovatko ne avoimen lähdekoodin, kaupallisia vai organisaation itse kehittämiä.

2.3. Tämän politiikan soveltamistapauksia ovat muun muassa:

2.3.1. testi- tai kehityskäyttöön tarkoitettujen tietoaineistojen valmistelu

2.3.2. tietojen siirtäminen analytiikkajärjestelmiin

2.3.3. toimittajien tai konsulttien pääsy operatiivisiin järjestelmiin

2.3.4. rekisteröityä koskevien tietojen minimointi käsittelyriskin vähentämiseksi

3. Tavoitteet

3.1. Varmistaa, ettei aitoja henkilötietoja tai muita arkaluonteisia tietoja paljasteta alemman tietoturvatason ympäristöissä silloin, kun ne eivät ole välttämättömiä.

3.2. Edellyttää peittämis- tai pseudonymisointimenetelmien käyttöä, kun aidot tunnisteet eivät ole tehtävän suorittamisen kannalta ehdottoman tarpeellisia.

3.3. Estää tietojen luvaton käyttö tai väärinkäyttö toteuttamalla tietojen muuntamiseen liittyvät kontrollit ennen tietojen siirtoa tai käsittelyä.

3.4. Varmistaa, että kaikki peittämis- ja pseudonymisointiprosessit ovat jäljitettävissä, todennettavissa ja toteutetaan hyväksytyillä työkaluilla.

3.5. Täyttää sovellettavat oikeudelliset ja sääntelyyn perustuvat vaatimukset, jotka koskevat tietojen minimointia, luottamuksellisuutta ja tietojen muuntamiseen liittyviä suojatoimia.

4. Roolit ja vastuut

4.1. Toimitusjohtaja

4.1.1. omistaa tämän politiikan ja hyväksyy sen

4.1.2. varmistaa, että kaikki osastot ja palveluntarjoajat noudattavat tietojen muuntamista koskevia vaatimuksia

4.1.3. katselmoi poikkeukset, riskienarvioinnit ja muunnoksia koskevat lokit

4.1.4. koordinoi oikeudelliset, operatiiviset tai toimittajiin liittyvät toimenpiteet rikkomustilanteissa

4.2. IT-tukipalveluntarjoaja / sisäinen IT

4.2.1. valitsee ja hallinnoi peittämis- tai pseudonymisointityökaluja

4.2.2. varmistaa, että asianmukaisia muuntamismenetelmiä käytetään tietotyypin perusteella

4.2.3. ylläpitää lokit muunnelluista tietoaineistoista ja avaintenhallintamenettelyistä

4.2.4. varmistaa, että peittäminen tehdään ennen testi-, toimittaja- tai analytiikkakäyttöä

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

9. Katselmointi- ja päivitysvaatimukset

9.1. Vuosittainen katselmointi

9.1.1. Toimitusjohtajan on katselmoitava tämä politiikka vähintään kerran vuodessa varmistaakseen, että siinä huomioidaan:

9.1.1.1. sovellettavan sääntelyn päivitykset (esim. EU:n GDPR, EU:n DORA-asetus)

9.1.1.2. uudet liiketoimintajärjestelmät tai tiedonsiirrot kolmansien osapuolten kanssa

9.1.1.3. auditointien tai peittämättömien tietojen käyttöön liittyvien poikkeamien palaute

9.2. Välikatselmoinnit

9.2.1. Katselmointi on tehtävä myös silloin, kun:

9.2.1.1. käyttöön otetaan uusia sovelluksia tai alustoja, jotka käsittelevät arkaluonteisia tietoja

9.2.1.2. merkittävä poikkeama paljastaa puutteita nykyisissä tietojen muuntamiseen liittyvissä kontrolleissa

9.2.1.3. luokittelutasojen muutokset vaikuttavat tietojen käsittelymenettelyihin

9.3. Versionhallinta ja muutoksenhallinta

9.3.1. Kaikkien politiikkamuutosten on:

9.3.1.1. oltava toimitusjohtajan hyväksymiä ja dokumentoitu muutoslokiin

9.3.1.2. oltava viestitty selkeästi niille työntekijöille ja palveluntarjoajille, joita muutos koskee

9.3.1.3. oltava arkistoitu turvallisesti siten, että vanhentuneisiin versioihin on rajoitettu pääsy

10. Liittyvät politiikat ja yhteydet

10.1. Tätä politiikkaa on sovellettava yhdessä seuraavien SME-politiikkojen kanssa, jotta arkaluonteisten tietojen suojaus on yhdenmukaista ja velvoittavaa:

10.1.1. P13S – Tiedon luokittelu- ja merkintäpolitiikka: Määrittää luokittelutasot (esim. Luottamuksellinen – henkilötieto), joiden perusteella päätetään, milloin peittämistä tai pseudonymisointia on käytettävä. Tämä politiikka toteuttaa tietojen muuntamista koskevat säännöt tiedon arkaluonteisuuden perusteella.

10.1.2. P14S – Tietojen säilytys- ja hävityspolitiikka: Varmistaa, että muunnellut tietoaineistot, mukaan lukien peitettyjä tai pseudonymisoituja tietoja sisältävät varmuuskopiot, säilytetään ja hävitetään sovellettavien sääntöjen mukaisesti, mukaan lukien yhdistämisavainten poistaminen, kun niitä ei enää tarvita.

10.1.3. P17S – Tietosuoja- ja yksityisyydensuojapolitiikka: Yhdenmukaistaa tietojen muuntamiskäytännöt laajempien tietosuojavelvoitteiden kanssa, mukaan lukien EU:n GDPR:n vaatimukset tietojen minimoinnista ja pseudonymisoinnin käytöstä henkilötietojen käsittelyn suojatoimena.

10.1.4. P30S – Tietoturvapoikkeamien hallintapolitiikka: Kattaa ilmoitus- ja eskalointimenettelyt tilanteissa, joissa tietoja paljastetaan luvattomasti, mukaan lukien peitettyjen tai pseudonymisoitujen tietojen epäasianmukainen käyttö tai palauttaminen.

10.1.5. P2S – Hallinnointirooleja ja vastuita koskeva politiikka: Määrittää kokonaisvastuun politiikan toteutuksesta, riskin hyväksynnästä ja poikkeusten hyväksynnästä ensisijaisesti toimitusjohtajalle.

10.2. Nämä politiikat muodostavat integroidun tietosuojan viitekehyksen ja varmistavat, että peittämistä ja pseudonymisointia koskevat toimenpiteet tukevat ISO 27001 -sertifiointia ja sääntelyvaatimusten mukaista toimintaa.

11. Viitestandardit ja viitekehykset

11.1. ISO/IEC 27001

11.1.1. Kohta 6.1.3: Edellyttää tietoturvariskien käsittelyä, mukaan lukien altistumisen vähentäminen tietojen muuntamismenetelmillä.

11.1.2. Kohta 8.1: Edellyttää sellaisten kontrollien toteuttamista, jotka ovat tarpeen tietoturvatavoitteiden saavuttamiseksi, mukaan lukien pseudonymisointi ja peittäminen.

11.2. ISO/IEC 27002

11.2.1. Kontrolli 8.11: Antaa ohjeistusta arkaluonteisten tietojen peittämisestä testi- ja kehitysjärjestelmissä.

11.2.2. Kontrolli 8.12: Tarjoaa keinoja tietovuotojen estämiseen hallitun muuntamisen ja pääsynhallinnan käytäntöjen avulla.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Varmistaa tietojen luottamuksellisuuden tietojen hämärtämisen avulla.

11.3.2. SC-28: Suojaa lepotilassa olevia ja käytössä olevia tietoja.

11.3.3. PT-2/PT-3: Edistävät tietosuojaa parantavien teknologioiden, mukaan lukien pseudonymisoinnin, käyttöä henkilötietojen käsittelyssä.

11.4. EU:n GDPR

11.4.1. Artikla 4(5): Määrittelee pseudonymisoinnin oikeudellisesti ja edellyttää yhdistämisavaimiin ja tunnisteisiin kohdistuvia hallintakeinoja.

11.4.2. Artikla 5(1)(c): Tukee tietojen minimoinnin periaatteita peittämisen avulla.

11.4.3. Artikla 32: Tunnistaa pseudonymisoinnin tekniseksi hallintakeinoksi, joka vähentää tietosuojariskejä.

11.5. EU:n NIS2-direktiivi

11.5.1. Artikla 21(2)(c): Edellyttää oikeasuhteisia teknisiä toimenpiteitä tietoturvariskin minimoimiseksi, mukaan lukien pseudonymisointi osana riskienhallintaa.

11.6. EU:n DORA-asetus

11.6.1. Artikla 10(1): Edellyttää ICT-riskien hallintakeinoja, joihin sisältyvät tietojen muuntamiseen liittyvät suojatoimet jatkuvuuden ja luottamuksellisuuden turvaamiseksi ulkoistamisen ja järjestelmäkehityksen aikana.

11.7. COBIT 2019

11.7.1. DSS05.01: Edellyttää tietovarojen suojaamista, mukaan lukien muuntaminen silloin, kun se on mahdollista.

11.7.2. DSS06.06: Edellyttää asianmukaisten hämärtämis- ja pseudonymisointimenetelmien käyttöä tietojen altistumisen rajoittamiseksi ympäristöissä, joissa luottamustaso on matalampi.