					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: P16					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 sääntelyn kanssa

Standardi/sääntely	Lauseke/artikla	Kommentti
ISO/IEC 27001:2022	Lauseke 6.1	Yleiset vaatimukset riskienhallinnalle sekä maskauksen ja pseudonymisoinnin operatiivisille kontrolleille
ISO/IEC 27002:2022	Kontrollit 8.11, 8	Kontrolliohjeistus maskauksen ja pseudonymisoinnin toteuttamiseen
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Tietosuojan ja luottamuksellisuuden kontrollit tietojen minimointiin, muuntamiseen ja pääsyn rajoittamiseen
EU:n GDPR	Artiklat 4(5), 5(1)(c,f), 32	Oikeusperusta ja vaatimukset pseudonymisoinnille sekä tietosuojatoimenpiteille
EU:n NIS2-direktiivi	Artikla 21(2)(c)	Velvoite teknisiin ja organisatorisiin toimenpiteisiin, mukaan lukien tietosuojaa parantavat teknologiat (PET)
EU:n DORA-asetus	Artiklat 10(1), 10(2)(e)	TVT-riskien hallinta sekä luottamuksellisuutta suojaavat kontrollit tietojen maskaukseen ja pseudonymisointiin
COBIT 2019	DSS05.01, DSS06.06, MEA	Hallintakontrollit tietosuojalle maskausta hyödyntäen sekä vaatimustenmukaisuuden arviointi

1. Tarkoitus

1.1 Tämä politiikka määrittää organisaation menettelytavat tietojen maskauksen ja pseudonymisoinnin toteuttamiseksi tietosuojaa parantavina teknologioina (PET), jotta henkilötietojen ja muiden arkaluonteisten tietojen tunnistettavuutta ja altistumista vähennetään.

1.2 Politiikka tukee tiedon turvallista käyttöä testauksessa, analytiikassa ja operatiivisessa toiminnassa sekä varmistaa lakisääteisten ja sääntelyyn perustuvien vaatimusten noudattamisen, lieventää tietoturvaloukkausten vaikutuksia ja toteuttaa minimoinnin ja luottamuksellisuuden periaatteita.

1.3 Politiikka on yhdenmukainen ISO/IEC 27001:2022 -standardin kanssa, tukee EU:n GDPR:n 4 artiklan 5 kohdan pseudonymisointia koskevia vaatimuksia ja integroi riskiperusteisen toteutuksen NIST-, NIS2-, DORA- ja COBIT 2019 -viitekehysten mukaisesti.

2. Soveltamisala

2.1 Tätä politiikkaa sovelletaan seuraaviin:

2.1.1 Kaikkiin työntekijöihin, urakoitsijoihin, kolmansiin osapuoliin ja toimittajiin, joilla on pääsy järjestelmiin, joissa käsitellään henkilötietoja, luottamuksellisia tietoja tai muita arkaluonteisia tietoja.

2.1.2 Kaikkiin tieto- ja käyttöympäristöihin, mukaan lukien tuotanto-, kehitys-, testaus- ja välivaiheen ympäristöt.

2.1.3 Kaikkiin tietojen maskauksen muotoihin (esim. staattinen, dynaaminen, deterministinen, tokenisointi) sekä pseudonymisointitekniikoihin, joita käytetään tietosuojariskien vähentämiseksi.

2.1.4 Kaikkiin tietotyyppeihin (rakenteinen tai rakenteeton tieto), järjestelmiin (omissa tiloissa tai pilvessä toimiviin järjestelmiin) ja sovelluksiin, joissa käsitellään henkilötietoja tai sääntelyn alaisia tietoja.

2.2 Soveltamisalaan sisältyy käyttö seuraavissa:

2.2.1 Sovelluskehitys- sekä laadunvarmistus- ja testausympäristöt

2.2.2 Analytiikka- tai raportointialustat

2.2.3 Tietojen vaihto kolmansien osapuolten tai kolmannen osapuolen palveluntarjoajien kanssa

2.2.4 Varmuuskopiointi-, arkistointi- tai palautusjärjestelmät

3. Tavoitteet

3.1 Varmistaa maskauksen ja pseudonymisoinnin yhdenmukainen ja tehokas soveltaminen tietojen altistumiseen tai väärinkäyttöön liittyvien riskien vähentämiseksi.

3.2 Varmistaa, että aitoja tietoja ei koskaan käytetä muissa kuin tuotantoympäristöissä, ellei niitä ole muunnettu hyväksytyillä PET-tekniikoilla.

3.3 Säilyttää viite-eheys, käytettävyys ja formaatin säilyttävät muunnokset silloin, kun niitä tarvitaan operatiivisen yhdenmukaisuuden varmistamiseksi.

3.4 Toteuttaa tiukka pääsynhallinta alkuperäisiin tietoihin, maskattuihin tietoihin ja uudelleentunnistamisen avaimiin.

3.5 Käsitellä maskattuja tai pseudonymisoituja tietoaineistoja arkaluonteisina tietoina, joihin sovelletaan käytön lokitusta, säilytyskontrolleja ja poikkeamien käsittelymenettelyjä.

3.6 Varmistaa näiden kontrollien tehokkuus jatkuvan testauksen, seurannan ja auditointimenettelyjen avulla.

4. Roolit ja vastuut

4.1 Ylin johto

4.1.1 Hyväksyy tämän politiikan ja varmistaa sen toimeenpanon osana laajempaa IT-hallintoa sekä tietosuojahankkeita.

4.2 Tietoturvajohtaja (CISO) / ISMS-päällikkö

4.2.1 Valvoo toteutusta ja jatkuvaa vaatimustenmukaisuutta.

4.2.2 Varmistaa yhdenmukaisuuden ISO/IEC 27001 -standardin lausekkeen 6.1.3 (riskien käsittely) ja lausekkeen 8.1 (operatiivinen ohjaus) kanssa.

4.2.3 Katselmoi lokit ja varmistaa kontrollien tehokkuuden.

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

9. Katselmointi- ja päivitysvaatimukset

9.1 Tämä politiikka on katselmoitava vähintään vuosittain tai aiemmin, jos tapahtuu jokin seuraavista:

9.1.1 Maskaukseen tai pseudonymisointiin vaikuttavat sääntelymuutokset

9.1.2 Uusien arkaluonteisia tietoja käsittelevien IT-järjestelmien käyttöönotto

9.1.3 Olennaiset muutokset organisaation tiedonluokittelumalliin

9.1.4 Auditointihavainnot, jotka osoittavat kontrollipuutteita

9.1.5 Uusien uhkien tai maskausteknologioiden ilmaantuminen

9.2 ISMS-päällikön on johdettava katselmointia yhteistyössä tietosuojavastaavan (DPO), tiedon omistajien, IT-tietoturvan sekä laki- ja compliance-toiminnon kanssa. Päivitysten on oltava versiohallittuja, ylimmän johdon hyväksymiä ja kaikille vaikutuksen alaisille sidosryhmille viestittyjä.

10. Liittyvät politiikat ja yhteydet

10.1 P13 - Tiedon luokittelu- ja merkintäpolitiikka. Maskausta ja pseudonymisointia koskevat päätökset perustuvat suoraan P13:ssa määriteltyyn tietokenttien luokitteluun ja arkaluonteisuustasoihin.

10.2 P14 - Tietojen säilytys- ja hävityspolitiikka. Muunnetut tietoaineistot on säilytettävä ja hävitettävä P14:n elinkaarisääntöjen mukaisesti siten, että maskattuja ja pseudonymisoituja tietoja käsitellään arkaluonteisina.

10.3 P17 - Tietosuoja- ja yksityisyydensuojapolitiikka. Määrittää tietosuojaperiaatteet ja sääntelyperustan pseudonymisoinnin soveltamiselle EU:n GDPR:n ja vastaavan lainsäädännön mukaisena käsittelytoimena.

10.4 P22 - Lokitus- ja valvontapolitiikka. Mahdollistaa maskaus- ja pseudonymisointitapahtumien keskitetyn auditoinnin ja hälytykset rakenteisten tietoturvavalvonnan protokollien mukaisesti.

11. Viitestandardit ja viitekehykset

11.1 ISO/IEC 27001

11.1.1 Lauseke 6.1.3 - riskienkäsittelysuunnitelma: määrittää maskauksen ja pseudonymisoinnin riskienkäsittelymekanismeiksi, joilla vähennetään arkaluonteisten tietojen tunnistettavuutta ei-välttämättömissä käsittely-ympäristöissä.

11.1.2 Lauseke 8.1 - operatiivinen suunnittelu ja ohjaus: edellyttää teknisiä ja menettelyllisiä suojatoimia tietojen turvalliseen muuntamiseen käsittelyn, säilytyksen tai siirron aikana.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollit 8.11, 8: ohjeistus tietojen maskaukseen ja pseudonymisointiin uudelleentunnistamisen ja tietovuotoriskien minimoimiseksi.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - henkilötietojen suojaaminen: tietosuojaa parantavien teknologioiden, kuten maskauksen ja pseudonymisoinnin, toteuttaminen.

11.3.2 PT-2, PT-3: henkilötietojen käsittelyn minimointi ja turvallisuus - muuntaminen tunnistettavuuden vähentämiseksi ja pääsynhallinnan toteuttamiseksi.

11.3.3 SC-12, SC-28, SC-30: tietojen luottamuksellisuus ja eheys - luottamuksellisuutta ja peittämistä koskevat kontrollit säilytyksessä, siirrossa ja käytössä.

11.4 EU:n GDPR (2016/679)

11.4.1 Artikla 4(5): pseudonymisoinnin virallinen määritelmä.

11.4.2 Artikla 32: käsittelyn turvallisuus - organisatoriset ja tekniset toimenpiteet pseudonymisoinnille.

11.4.3 Artikla 5(1)(c,f): tietojen minimointi ja luottamuksellisuus pseudonymisoinnin ja maskauksen avulla.

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

11.5.1 Artikla 21(2)(c): edellyttää PET-teknologioita, kuten maskausta ja pseudonymisointia, osana tietoturvatoimenpiteitä.

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

11.6.1 Artikla 10(1): TVT-riskienhallinnan viitekehys sisältää maskaus- ja pseudonymisointikontrollit.

11.6.2 Artikla 10(2)(e): edellyttää muunnosteknologioiden käyttöä henkilötietojen ja taloudellisten tietojen suojaamiseksi.

11.7 COBIT 2019

11.7.1 DSS05.01: tietovarojen suojaaminen - maskausta ja pseudonymisointia koskevat vaatimukset.

11.7.2 DSS06.06: turvallinen testaus ja analytiikka - maskaus tuotantoympäristön ulkopuolisissa ympäristöissä.

11.7.3 MEA03: vaatimustenmukaisuuden seuranta maskauksen ja pseudonymisoinnin tehokkuuden varmistamiseksi.