					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII16					Asiakirjan nimi: **Tietosuojakoulutuksen, tietoisuuden ja pätevyyden 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 säädösten kanssa

Standardi / säädös	Lauseke / hallintakeino / artikla	Sovellettavuus	Kattavuuden tyyppi	Kommentti
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Pätevyys ja tietoisuus
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Viestintä ja dokumentoitu näyttö
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operatiivinen ohjaus, mittaaminen ja parantaminen
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Henkilötietojen käsittelyä koskeva tietoisuus, opetus ja koulutus
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Osoitusvelvollisuus, henkilötietojen käsittelijän hallinnointi, turvallisuus ja tietosuojavastaavan tehtävät
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Pätevyys, tietoisuus ja koulutus
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Tietoisuutta, opetusta ja koulutusta koskeva ohjeistus
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Tietoturva ja tietosuojan noudattaminen

1. Soveltamisala

1.1 Tämä politiikka määrittää organisaation vaatimukset henkilötietojen hallintajärjestelmän tietosuojakoulutukselle, tietoisuudelle ja pätevyydelle.

1.2 Tätä politiikkaa sovelletaan henkilöstöön, sopimuskumppaneihin, määräaikaisiin työntekijöihin, olennaisiin kolmansiin osapuoliin, henkilötietojen käsittelijöihin, alikäsittelijöihin ja muihin sidosryhmiin, joiden työ voi vaikuttaa henkilötietojen käsittelyyn, PIMS:n suorituskykyyn, rekisteröidyn oikeuksiin, tietosuojariskiin, henkilötietoihin liittyvään tietoturvaan, henkilötietojen käsittelijän ohjeisiin, henkilötietopoikkeamiin, dokumentoituun tietoon tai vaatimustenmukaisuutta koskevaan näyttöön.

1.3 Tätä politiikkaa sovelletaan rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän tilanteisiin.

1.4 Tämä politiikka kattaa:

1.4.1 tietosuojakoulutuksen kohderyhmien tunnistamisen;

1.4.2 perehdytyskoulutuksen;

1.4.3 vuosittaisen kertauskoulutuksen;

1.4.4 roolipohjaisen ja tapahtumaperusteisen koulutuksen;

1.4.5 koulutuksen suorittamista koskevan näytön;

1.4.6 suorittamatta jäämisen eskaloinnin;

1.4.7 koulutuksen vaikuttavuuden katselmoinnin;

1.4.8 henkilötietojen käsittelijän, alikäsittelijän ja kolmannen osapuolen koulutuksen varmentamisnäytön.

1.5 Tämä politiikka ei luo erillistä koulutusmatriisia, koulutusmittaristoa, henkilöstöhallinnon rekisteriä, pätevyysrekisteriä, kurinpitorekisteriä tai asiakaskoulutusrekisteriä. Koulutustehtävät, suoritukset, muistutukset, pätevyyttä koskeva näyttö ja tietoisuutta koskeva näyttö kirjataan REG11:een, ja poikkeukset, eskaloinnit, poikkeamat, korjaavat toimenpiteet ja katselmointinäyttö kirjataan REG12:een. Henkilötietojen käsittelijän, alikäsittelijän ja kolmannen osapuolen koulutuksen varmentamisnäyttö kirjataan tarvittaessa REG08:aan.

1.6 Tämä politiikka ei toista:

1.6.1 roolien vastuun määrittämistä PII02:ssa;

1.6.2 käsittelytoimien luetteloa ja oikeusperustetta koskevia vaatimuksia PII03:ssa;

1.6.3 tietosuojariskien ja DPIA:n menetelmää PII07:ssa;

1.6.4 sisäänrakennetun tietosuojan portteja PII08:ssa;

1.6.5 henkilötietojen käsittelijän elinkaaren hallinnointia PII12:ssa;

1.6.6 henkilötietojen tietoturvan ja pääsynhallinnan toimintaa PII14:ssa;

1.6.7 henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten työnkulkua PII15:ssa;

1.6.8 dokumentoidun tiedon hallinnointia PII17:ssa;

1.6.9 seurannan, sisäisen tarkastuksen ja parantamisen hallinnointia PII18:ssa.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että henkilötietojen käsittelyyn vaikuttavaa työtä tekevät henkilöt ymmärtävät tietosuojavastuunsa, suorittavat asianmukaisen koulutuksen määritetyssä aikataulussa, ylläpitävät roolinsa kannalta olennaista pätevyyttä ja tuottavat todennettavissa olevaa näyttöä koulutuksesta, tietoisuudesta ja eskaloinnista.

2.2 Tämä politiikka tukee PIMS:n yhdenmukaista toteutusta käyttämällä REG11:tä ensisijaisena koulutuksen ja tietoisuuden näyttöobjektina sekä REG08:aa, REG10:tä ja REG12:ta tukevina näyttöobjekteina.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää tietosuojakoulutuksen kohderyhmät;

3.1.2 määrittää perehdytyskoulutuksen vaatimukset;

3.1.3 määrittää vuosittaisen kertauskoulutuksen vaatimukset;

3.1.4 määrittää roolipohjaisen tietosuojakoulutuksen vaatimukset;

3.1.5 kirjata suoritusta koskeva näyttö REG11:een;

3.1.6 eskaloida suorittamatta jääminen REG12:n kautta;

3.1.7 ylläpitää tarvittaessa henkilötietojen käsittelijän, alikäsittelijän ja kolmannen osapuolen koulutuksen varmentamisnäyttöä REG08:ssa;

3.1.8 katselmoida koulutuksen vaikuttavuutta ilman liiallisia mittareita tai päällekkäisiä rekistereitä;

3.1.9 varmistaa, että koulutussisältö pysyy yhdenmukaisena voimassa olevien PIMS-politiikkojen ja olennaisten tietosuojavelvoitteiden kanssa.

4. Politiikkalausumat

4.1 Koulutuksen kohderyhmä ja osoittaminen

4.1.1 [All] Privacy Lead / PIMS Manager ON määritettävä PIMS-koulutuksen kohderyhmäluokat REG11:ssä ennen kunkin vuosittaisen koulutussyklin alkamista.

4.1.2 [All] Process Owner / Business Owner ON tunnistettava henkilöstö, jonka tehtäviin kuuluu henkilötietojen käsittely, REG11:ssä ennen perehdytystä, roolin osoittamista tai olennaista tehtävämuutosta.

4.1.3 [Conditional] System Owner / Application Owner ON tunnistettava käyttäjät, jotka tarvitsevat henkilötietojärjestelmiä, etuoikeutettuja käyttöoikeuksia tai hallinnollista tietosuojakoulutusta, REG11:ssä ennen käyttöoikeuden käyttöönottoa tai sen olennaista muuttamista.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager ON kirjattava yhteisrekisterinpitäjien koulutusvastuun jako REG11:een tai REG08:aan ennen yhteisen käsittelytoimen aloittamista tai sen olennaista muuttamista.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor ON tunnistettava tehostetun tietosuojakoulutuksen tarpeet REG11:ssä ennen koulutuksen osoittamista rooleille, jotka käsittelevät korkean riskin käsittelyä, erityisiin henkilötietoryhmiin kuuluvia henkilötietoja, rekisteröidyn oikeuksia, DPIA-arviointeja, henkilötietojen kansainvälisiä siirtoja tai tietoturvaloukkauksen arviointia.

4.1.6 [All] Privacy Lead / PIMS Manager ON kirjattava osoitettu koulutuksen kohderyhmä, koulutustyyppi, vaadittu suorituspäivä ja näytön omistaja REG11:een ennen kunkin vuosittaisen koulutussyklin alkamista.

4.2 Perehdytys ja vuosittaisen koulutuksen aikataulu

4.2.1 [All] Privacy Lead / PIMS Manager ON osoitettava perustason tietosuojatietoisuuskoulutus REG11:ssä 10 työpäivän kuluessa perehdytyksestä henkilöstölle, jolla on pääsy henkilötietoihin tai PIMS-vastuita.

4.2.2 [All] Process Owner / Business Owner ON varmistettava, että nimetty henkilöstö suorittaa perehdytyksen tietosuojakoulutuksen REG11:ssä ennen valvomattoman pääsyn hyväksymistä henkilötietoihin tai 30 päivän kuluessa perehdytyksestä sen mukaan, kumpi ajankohta on aikaisempi.

4.2.3 [All] Privacy Lead / PIMS Manager ON osoitettava vuosittainen tietosuojan kertauskoulutus REG11:ssä vähintään kerran 12 kuukaudessa.

4.2.4 [All] Process Owner / Business Owner ON vahvistettava nimetyn henkilöstön vuosittaisen kertauskoulutuksen suoritustila REG11:ssä julkaistuun vuosittaiseen määräpäivään mennessä.

4.2.5 [Conditional] Privacy Lead / PIMS Manager ON osoitettava kohdennettu kertauskoulutus REG11:ssä 30 päivän kuluessa olennaisesta tietosuojapolitiikan muutoksesta, olennaisesta PIMS-prosessin muutoksesta, auditointihavainnosta, toistuvasta koulutuksen epäonnistumisesta tai asiaankuuluvasta henkilötietopoikkeamasta saadusta opista.

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

9. Poikkeukset

9.1.1 [All] Process Owner / Business Owner ON kirjattava tietosuojakoulutusta koskeva poikkeuspyyntö REG12:een ennen vaaditun suoritusmääräajan pidentämistä.

9.1.2 [All] Privacy Lead / PIMS Manager ON hyväksyttävä tai hylättävä tietosuojakoulutusta koskevat poikkeuspyynnöt REG12:ssa ennen poikkeuksen aktivoitumista.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ON annettava neuvoja koulutuspoikkeuksista REG12:ssa ennen hyväksyntää, kun poikkeus vaikuttaa korkean riskin käsittelyyn, erityisiin henkilötietoryhmiin kuuluviin henkilötietoihin, oikeuksien käsittelyyn, poikkeamien käsittelyyn, henkilötietojen kansainvälisiin siirtoihin tai sertifiointinäyttöön.

9.1.4 [Conditional] Top Management ON hyväksyttävä tietosuojakoulutuksen poikkeukset REG12:ssa ennen aktivointia, kun poikkeus vaikuttaa toistuvaan suorittamatta jäämiseen, etuoikeutettuun pääsyyn henkilötietoihin, vaikutuksiltaan merkittävään henkilötietojen käsittelyyn tai viranomaisille esitettävään näyttöön.

9.1.5 [All] Privacy Lead / PIMS Manager ON määritettävä poikkeuksen omistaja, päättymispäivä, kompensoiva toimenpide ja katselmointipäivä REG12:ssa ennen minkään tietosuojakoulutusta koskevan poikkeuksen hyväksymistä.

9.1.6 [All] Process Owner / Business Owner ON suljettava tai uusittava hyväksytyt tietosuojakoulutuksen poikkeukset REG12:ssa ennen poikkeuksen päättymispäivää.

10. Soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager ON kirjattava koulutukseen liittyvä poikkeama REG12:een viiden työpäivän kuluessa, kun pakollisen tietosuojakoulutuksen näyttö puuttuu, on puutteellinen, myöhässä tai ei ole jäljitettävissä REG11:een.

10.1.2 [All] Process Owner / Business Owner ON varmistettava, että myöhässä oleva pakollinen tietosuojakoulutus suoritetaan tai eskaloidaan REG11:ssä tai REG12:ssa 10 työpäivän kuluessa myöhässä-tilan kirjaamisesta.

10.1.3 [Conditional] System Owner / Application Owner ON rajoitettava uutta vaikutuksiltaan merkittävää pääsyä henkilötietoihin REG12:ssa, kun vaadittu perehdytys- tai roolipohjainen tietosuojakoulutus on edelleen suorittamatta eskaloinnin jälkeen.

10.1.4 [Processor] Vendor / Procurement Owner ON eskaloitava puuttuva henkilötietojen käsittelijän, alikäsittelijän tai ulkoisen työvoiman koulutuksen varmentamisnäyttö REG08:ssa ja REG12:ssa viiden työpäivän kuluessa tunnistamisesta.

10.1.5 [Conditional] Incident Response Coordinator ON linkitettävä koulutukseen liittyvät soveltamistoimet REG10:een yhden työpäivän kuluessa, kun koulutuksen epäonnistuminen myötävaikutti epäiltyyn tai vahvistettuun henkilötietopoikkeamaan.

10.1.6 [All] Internal Audit / Compliance Reviewer ON todennettava koulutuksen korjaavien toimenpiteiden sulkemisnäyttö REG12:ssa seuraavassa suunnitellussa auditoinnissa tai 60 päivän kuluessa sulkemisesta sen mukaan, kumpi ajankohta on aikaisempi.

11. Katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager ON katselmoitava tämä politiikka ja koulutussisältö vähintään vuosittain ja kirjattava katselmoinnin tulos REG11:een tai REG12:een.

11.1.2 [All] Privacy Lead / PIMS Manager ON katselmoitava tämä politiikka 30 päivän kuluessa olennaisesta muutoksesta PIMS:n soveltamisalaan, tietosuojalainsäädäntöön, käsittelytoimiin, roolimalliin, poikkeamaoppeihin, auditointihavaintoihin tai koulutuksen vaikuttavuuden tuloksiin.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor ON katselmoitava tietosuojan kannalta merkittävät politiikkamuutokset REG12:ssa ennen hyväksyntää.

11.1.4 [All] Top Management ON hyväksyttävä olennaiset muutokset tähän politiikkaan REG12:ssa ennen julkaisua.

11.1.5 [All] Privacy Lead / PIMS Manager ON päivitettävä REG11:n koulutussisältö ja tehtävien osoittamista koskeva näyttö 30 päivän kuluessa hyväksytystä olennaisesta politiikkamuutoksesta.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tulee lukea yhdessä seuraavien kanssa:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka;

12.3 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka;

12.4 PII03 - Henkilötietojen käsittelytoimien luettelon ja oikeusperusteen politiikka;

12.5 PII04 - Tietosuojaselosteen ja läpinäkyvyyden politiikka;

12.6 PII05 - Suostumuksen ja valinta-asetusten hallinnan politiikka;

12.7 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka;

12.8 PII07 - Tietosuojariskien arvioinnin ja DPIA:n politiikka;

12.9 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka;

12.10 PII09 - Henkilötietojen keräämisen, käytön, luovutuksen ja jakamisen politiikka;

12.11 PII10 - Henkilötietojen säilytyksen, poistamisen ja hävittämisen politiikka;

12.12 PII12 - Henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojahallinnan politiikka;

12.13 PII13 - Henkilötietojen kansainvälisten siirtojen politiikka;

12.14 PII14 - Henkilötietojen tietoturva- ja pääsynhallintapolitiikka;

12.15 PII15 - Henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallintapolitiikka;

12.16 PII17 - PIMS:n dokumentoidun tiedon ja näytön hallintapolitiikka;

12.17 PII18 - PIMS:n seuranta-, auditointi- ja parantamispolitiikka.

13. Viitestandardit ja viitekehykset

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].