					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII17					Asiakirjan nimi: **PIMS:n dokumentoidun tiedon ja todentavan aineiston hallintapolitiikka**							
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	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA:n dokumentoitu tieto
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS:n dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operatiivisen todentavan aineiston hallinta
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Seurannan todentava aineisto
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Auditointinäyttö
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Johdon katselmoinnin todentava aineisto
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Poikkeaman ja korjaavien toimenpiteiden todentava aineisto
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Rekisterinpitäjän käsittelytallenteet
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Henkilötietojen käsittelijän sopimuksia ja ohjeita koskeva todentava aineisto
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Tallenteiden suojaus
GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuuden todentava aineisto
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän toimenpiteet ja todentava aineisto
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijää koskeva dokumentaatio
GDPR	Article 30	Both	Supporting	Käsittelyä koskevat tallenteet
GDPR	Article 32	Both	Supporting	Todentavan aineiston suojaus

ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Tietosuojan noudattamisen todentava aineisto
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Tallenteiden suojaus
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Dokumentoidun tiedon hallinta
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Tallenteiden suojaus
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Yksityisyyden ja PII:n suojaus

1. Soveltamisala

1.1 Tässä politiikassa määritetään pakolliset vaatimukset PIMS:n dokumentoidun tiedon luomiselle, hyväksymiselle, versionhallinnalle, suojaamiselle, säilyttämiselle, hakemiselle, kääntämiselle, käytöstä poistamiselle ja todentamiselle.

1.2 Tätä politiikkaa sovelletaan PIMS-politiikkoihin, rekistereihin, dokumentoituihin hyväksyntöihin, todentavan aineiston tallenteisiin, auditointinäyttöön, johdon katselmoinnin tallenteisiin, korjaavien toimenpiteiden todentavaan aineistoon sekä hallittuihin käännöksiin, joita käytetään PIMS-vaatimustenmukaisuuden osoittamiseen.

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

1.4 Tämä politiikka ei luo erillistä asiakirjahallinnan rekisteriä. Dokumentoidun tiedon hallinnan todentavaa aineistoa ylläpidetään kanonisten PIMS-näyttöobjektien REG01–REG12 kautta, ja REG03:a ja REG12:a käytetään hallintakeinojen sovellettavuuteen, auditointiin, poikkeamiin, korjaaviin toimenpiteisiin ja parantamiseen liittyvään todentavaan aineistoon.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että PIMS:n dokumentoitu tieto on täsmällistä, hallittua, valtuutettujen käyttäjien saatavilla, suojattu luvattomalta muuttamiselta tai luovuttamiselta, säilytetty auditoitavuutta varten ja poistettu käytöstä, kun se on vanhentunut.

2.2 Tämä politiikka tukee valmiutta auditointia varten varmistamalla, että PIMS-vaatimustenmukaisuuden osoittamiseen tarvittava todentava aineisto voidaan paikantaa, varmentaa, hakea ja yhdistää sovellettaviin politiikkoihin, hallintakeinoihin, käsittelytoimiin, riskeihin, auditointeihin ja korjaaviin toimenpiteisiin.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää PIMS:n dokumentoidun tiedon hallintavaatimukset;

3.1.2 ylläpitää todentavan aineiston eheyttä REG01–REG12-kokonaisuudessa;

3.1.3 varmistaa, että politiikkojen ja todentavan aineiston hyväksyntä on jäljitettävissä;

3.1.4 varmistaa, että versiohistoria ja käytöstä poistamista koskevat päätökset dokumentoidaan;

3.1.5 yhdistää PIMS:n todentava aineisto soveltuvuuslausuntoon ja politiikkakartoituksiin;

3.1.6 hallita pääsyä PIMS-asiakirjoihin ja todentavan aineiston tallenteisiin;

3.1.7 tukea monikielisten politiikkojen ja todentavan aineiston versionhallintaa;

3.1.8 mahdollistaa auditointinäytön oikea-aikainen hakeminen;

3.1.9 ehkäistä tarpeetonta asiakirjahallinnan byrokratiaa;

3.1.10 säilyttää auditointia varten valmiit tallenteet sertifiointia, asiakkaiden varmentamista ja jatkuvaa parantamista varten.

4. Politiikkalausumat

4.1 PIMS:n dokumentoidun tiedon hallinta

4.1.1 [All] Rooli Privacy Lead / PIMS Manager on velvollinen ylläpitämään PIMS:n dokumentoidun tiedon indeksiä REG12:ssa ennen PIMS:n ensimmäistä julkaisua ja sen jälkeen neljännesvuosittain.

4.1.2 [All] Rooli Process Owner / Business Owner on velvollinen tunnistamaan kunkin omistamansa PII:n käsittelytoimen edellyttämän dokumentoidun tiedon REG02:ssa ennen käsittelytoimen aloittamista ja sen jälkeen vuosittain.

4.1.3 [All] Rooli Privacy Lead / PIMS Manager on velvollinen liittämään sovellettavat PIMS-politiikat, hallintakeinot ja todentavaa aineistoa koskevat velvoitteet REG03:een ennen jokaista

politiikkajulkaisua ja 15 työpäivän kuluessa olennaisesta hallintakeinon sovellettavuuden muutoksesta.

4.1.4 [All] Rooli Privacy Lead / PIMS Manager on velvollinen osoittamaan pääsytason ja todentavan aineiston arkaluonteisuusluokituksen kullekin PIMS:n dokumentoidun tiedon luokalle REG12:ssa ennen luokan käyttöönottoa.

4.2 Luominen, hyväksyntä, versionhallinta ja julkaisu

4.2.1 [All] Rooli Privacy Lead / PIMS Manager on velvollinen määrittämään asiakirjan tunnisteen, omistajan, versionumeron, hyväksyntätilan, voimaantulopäivän ja katselmointipäivän REG12:ssa ennen PIMS:n dokumentoidun tiedon julkaisemista.

4.2.2 [All] Rooli Top Management on velvollinen hyväksymään keskeiset PIMS-politiikat ja olennaiset politiikkamuutokset REG12:ssa ennen julkaisemista.

4.2.3 [All] Rooli Privacy Lead / PIMS Manager on velvollinen hyväksymään PIMS:n todentavan aineiston mallipohjat tai rekistereihin sisällytetyt osiot REG12:ssa ennen operatiivista käyttöä.

4.2.4 [All] Rooli Privacy Lead / PIMS Manager on velvollinen kirjaamaan versiohistorian ja muutoksen perustelut REG12:ssa ennen päivitetyn PIMS:n dokumentoidun tiedon julkaisemista.

4.2.5 [All] Rooli Privacy Lead / PIMS Manager on velvollinen kirjaamaan hyväksytyistä PIMS:n dokumentoidun tiedon muutoksista viestimisen REG11:een 30 päivän kuluessa julkaisemisesta.

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

9. Poikkeukset

9.1.1 [All] Rooli Process Owner / Business Owner on velvollinen pyytämään dokumentoitua tietoa tai todentavan aineiston hallintaa koskevat poikkeukset REG12:ssa ennen tästä politiikasta poikkeamista.

9.1.2 [All] Rooli Privacy Lead / PIMS Manager on velvollinen arvioimaan kunkin dokumentoitua tietoa tai todentavan aineiston hallintaa koskevan poikkeuksen REG12:ssa 10 työpäivän kuluessa pyynnöstä.

9.1.3 [All] Rooli Data Protection Officer / Privacy Advisor on velvollinen kirjaamaan neuvonsa REG12:een ennen sellaisen poikkeuksen hyväksymistä, joka koskee PII:tä sisältävän todentavan aineiston luovuttamista, käännöseroa, säilytysristiriitaa tai auditointinäytön rajoitusta.

9.1.4 [All] Rooli Top Management on velvollinen hyväksymään yli 30 päivää kestävät tai sertifiointiin, korkean riskin käsittelyyn tai ulkoiseen varmentamiseen vaikuttavat dokumentoidun tiedon poikkeukset REG12:ssa ennen poikkeuksen voimaantuloa.

9.1.5 [All] Rooli Privacy Lead / PIMS Manager on velvollinen asettamaan REG12:ssa kullekin hyväksytylle dokumentoitua tietoa tai todentavan aineiston hallintaa koskevalle poikkeukselle enintään 90 päivän päättymispäivän.

9.1.6 [All] Rooli Privacy Lead / PIMS Manager on velvollinen sulkemaan tai arvioimaan uudelleen kunkin dokumentoitua tietoa tai todentavan aineiston hallintaa koskevan poikkeuksen REG12:ssa viiden työpäivän kuluessa sen päättymisestä.

10. Soveltaminen

10.1.1 [All] Rooli Privacy Lead / PIMS Manager on velvollinen kirjaamaan puuttuvan, epätarkan, hallitsemattoman, vanhentuneen tai hakukelvottoman PIMS:n dokumentoidun tiedon poikkeamana REG12:een viiden työpäivän kuluessa sen tunnistamisesta.

10.1.2 [All] Rooli Privacy Lead / PIMS Manager on velvollinen estämään PIMS:n dokumentoidun tiedon julkaisemisen, kun vaadittua hyväksyntää, versiota, omistajaa tai voimaantulopäivää koskeva todentava aineisto puuttuu REG12:sta.

10.1.3 [All] Rooli Process Owner / Business Owner on velvollinen estämään käsittelyä koskevan todentavan aineiston toimittamisen auditointiin, jos vaadittua omistajaa, päivämäärää, tilaa tai hyväksyntää koskeva todentava aineisto puuttuu REG02:sta.

10.1.4 [All] Rooli System Owner / Application Owner on velvollinen poistamaan luvattoman pääsyn PIMS:n dokumentoidun tiedon tietovarastoihin ja kirjaamaan poistamisen REG12:een yhden työpäivän kuluessa tunnistamisesta.

10.1.5 [All] Rooli Internal Audit / Compliance Reviewer on velvollinen varmentamaan dokumentoidun tiedon poikkeamia koskevien korjaavien toimenpiteiden vaikuttavuuden REG12:ssa seuraavassa aikataulutetussa auditoinnissa tai 60 päivän kuluessa sulkemisesta sen mukaan, kumpi tapahtuu ensin.

11. Katselmointi ja ylläpito

11.1.1 [All] Rooli Privacy Lead / PIMS Manager on velvollinen katselmoimaan tämän politiikan vuosittain ja 30 päivän kuluessa PIMS:n dokumentoidun tiedon vaatimusten olennaisesta muutoksesta.

11.1.2 [All] Rooli Privacy Lead / PIMS Manager on velvollinen katselmoimaan tämän politiikan 30 päivän kuluessa merkittävästä auditointihavainnosta, sertifioinnin poikkeamasta, tietovarastoalustan muutoksesta tai monikielisen julkaisuprosessin muutoksesta.

11.1.3 [All] Rooli Data Protection Officer / Privacy Advisor on velvollinen katselmoimaan tähän politiikkaan tehtävät tietosuojan kannalta merkittävät muutokset REG12:ssa ennen hyväksyntää.

11.1.4 [All] Rooli Top Management on velvollinen hyväksymään tämän politiikan olennaiset muutokset REG12:ssa ennen julkaisua.

11.1.5 [All] Rooli Privacy Lead / PIMS Manager on velvollinen kirjaamaan tämän politiikan hyväksytyistä muutoksista viestimisen REG11:een 30 päivän kuluessa julkaisusta.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.3 PII02 - Yksityisyydensuojan rooleja, vastuita ja osoitusvelvollisuutta koskeva politiikka

12.4 PII03 - PII:n käsittelytoimien luetteloa ja oikeusperustetta koskeva politiikka

12.5 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.6 PII05 - Suostumuksen ja valinta-asetusten hallintapolitiikka

12.7 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.8 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.9 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.10 PII09 - PII:n keräämistä, käyttöä, luovuttamista ja jakamista koskeva politiikka

12.11 PII10 - PII:n säilytys-, poisto- ja hävityspolitiikka

12.12 PII11 - PII:n täsmällisyys- ja laatupolitiikka

12.13 PII12 - Henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojahallinnan politiikka

12.14 PII13 - PII:n kansainvälisen siirron politiikka

12.15 PII14 - PII:n turvallisuus- ja pääsynhallintapolitiikka

12.16 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.17 PII16 - Tietosuojakoulutus-, tietoisuus- ja osaamispolitiikka

12.18 PII18 - PIMS:n seuranta-, auditointi- ja parantamispolitiikka

13. Viitestandardit ja viitekehykset

13.1 Tämä politiikka on kartoitettu seuraaviin standardeihin ja säädöksiin. Kartoitus selittää, miten politiikka tukee viitattuja vaatimuksia, ja tunnistaa sisäiset lausekkeet, joilla ne toteutetaan tai joita ne tukevat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Kartoitettu PIMS:n soveltuvuuslausunnon, hallintakeinojen sovellettavuustallenteiden sekä politiikkojen ja todentavan aineiston välisen liitoksen ylläpitämiseen. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Kartoitettu dokumentoidun tiedon tunnistamiseen, hyväksyntään, versionhallintaan, pääsyyn, hakemiseen, säilyttämiseen, käytöstä poistamiseen, käännösversioiden liitokseen ja säilytysmetatietoihin. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Kartoitettu operatiivisen suunnittelun ja hallinnan todentavaan aineistoon käsittelytallenteiden, todentavan aineiston mallipohjien, operatiivisen todentavan aineiston laadun ja ulkoisesti toimitetun todentavan aineiston osalta. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Kartoitettu dokumentoidun todentavan aineiston ylläpitämiseen mittaamisesta, hakusuorituskyvystä, todentavan aineiston puutteista, käännösten eroavuuksista ja tietovarastojen käyttöoikeuskatselmoinnin valmistumisesta. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Kartoitettu auditointinäytön hakemiseen, auditointiotantaan, auditointinäytön jäljitettävyyteen ja dokumentoidun tiedon hallintaan liittyviin auditointihavaintoihin. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Kartoitettu johdon katselmoinnin todentavaan aineistoon, dokumentoidun tiedon hallinnan käsittelyyn johdon katselmoinnissa sekä Top Management -tason katselmointiin todentavan aineiston hallinnan suorituskyvystä. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Kartoitettu dokumentoidun tiedon poikkeamiin, korjaaviin toimenpiteisiin, poikkeusten käsittelyyn, sulkemiseen ja vaikuttavuuden varmentamiseen. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Kartoitettu rekisterinpitäjän käsittelytallenteisiin, osoitusvelvollisuuden dokumentaatioon, käsittelyä koskevan todentavan aineiston laatuun sekä rekisterinpitäjän velvoitteita tukevan todentavan aineiston säilyttämiseen. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Kartoitettu henkilötietojen käsittelijän sopimukseen, asiakkaan ohjeeseen, ulkoisesti toimitettuun todentavaan aineistoon ja henkilötietojen käsittelijäsuhteiden todentavan aineiston hallintaan. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Kartoitettu PIMS-tallenteiden suojaamiseen katoamiselta, luvattomalta muuttamiselta, luvattomalta pääsyltä, luvattomalta luovuttamiselta ja virheelliseltä hävittämiseltä. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartoitettu osoitusvelvollisuuden todentavaan aineistoon, todentavan aineiston jäljitettävyyteen, todentavan aineiston hakemiseen, poikkeamatallenteisiin ja vaatimustenmukaisuutta osoittaviin auditointivalmiisiin tallenteisiin. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän hallinnointia koskevaan todentavaan aineistoon, hyväksyntätallenteisiin, politiikkojen hallintaan, osoitusvelvollisuustoimenpiteisiin, dokumentoituun katselmointiin ja Top Management -valvontaan. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Kartoitettu henkilötietojen käsittelijöitä ja alikäsittelijöitä koskevaan dokumentaatioon, asiakkaan ohjeita koskevaan todentavaan aineistoon, ulkoisesti toimitettuun prosessitodentavaan aineistoon ja todentavan aineiston luovuttamisen hallintaan. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Kartoitettu käsittelytallenteiden todentavaan aineistoon, todentavan aineiston laatuvaatimuksiin, käsittelytoimien viitteisiin sekä käsittelyä koskevan todentavan aineiston omistaja- ja tilametatietoihin. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Kartoitettu todentavan aineiston tietovarastojen suojaamiseen, pääsyrajoituksiin, pääsyhyväksyntöihin, tietovarastojen suojauksen katselmointiin ja luvattoman pääsyn poistamiseen. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Kartoitettu tietosuojan noudattamisen todentavaan aineistoon, auditointinäytön hakemiseen, todentavan aineiston jäljitettävyyteen, riippumattoman arvioinnin tukemiseen ja korjaavien toimenpiteiden todentavaan aineistoon. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Kartoitettu PII:hin liittyvien tallenteiden suojaamiseen, tallenteiden säilyttämiseen sekä todentavan aineiston tietovarastojen pääsyn ja poistamisen hallintaan. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Kartoitettu dokumentoidun tiedon tunnistamiseen, hyväksyntään, saatavuuteen, suojaamiseen, versionhallintaan, säilyttämiseen, käytöstä poistamiseen sekä ulkoisesti vaaditun dokumentoidun tiedon hallintaan. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Kartoitettu PIMS-tallenteiden suojaamiseen katoamiselta, tuhoutumiselta, väärentämiseltä, luvattomalta pääsyltä, luvattomalta luovuttamiselta ja virheelliseltä hävittämiseltä. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Kartoitettu yksityisyyden ja PII:n suojaamiseen dokumentoidussa tiedossa, todentavan aineiston tietovarastoissa, luovutuksissa ja pääsyhallituissa tallenteissa. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].