					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII01					Asiakirjan nimi: **Henkilötietojen hallintajärjestelmän 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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Toimintaympäristön ja PIMS-roolin määrittäminen
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Sidosryhmät ja vaatimukset
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS:n soveltamisala
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	PIMS:n perustaminen ja parantaminen
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Johtajuus ja sitoutuminen
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Tietosuojapolitiikka
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roolit ja valtuudet
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riskit ja mahdollisuudet
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Tietosuojariskien arviointi
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tietosuojariskien käsittely ja SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Tietosuojatavoitteet
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Suunnitellut PIMS-muutokset
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resurssit
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Pätevyys
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Tietoisuus
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Viestintä
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operatiivinen suunnittelu ja ohjaus

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operatiivinen tietosuojariskien arviointi
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operatiivinen tietosuojariskien käsittely
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Seuranta ja arviointi
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Sisäinen tarkastus
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Johdon katselmointi
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Jatkuva parantaminen
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Poikkeama ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Rekisterinpitäjän hallinnointitallenteet
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Henkilötietojen käsittelijän sopimus ja tarkoitukset
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Yhteys PII:n turvallisuutta koskevaan politiikkaan
GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuutta koskeva näyttö
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän toimenpiteet ja politiikka
GDPR	Article 26	Joint Controller	Supporting	Yhteisrekisterinpitäjien järjestelyt
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijöiden hallinnointi
GDPR	Article 30	Both	Supporting	Käsittelytoimia koskevat tallenteet
GDPR	Article 32	Both	Supporting	Käsittelyn turvallisuus
GDPR	Article 35	Controller	Supporting	DPIA-hallinnointi
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1;	Both	Supporting	Tietosuojakontrollit ja -periaatteet

	Clause 5.11; Clause 5.12			
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-prosessi ja valmistelu
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII:n suojausohjelma ja politiikka
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Organisaation tietosuojariskien integrointi

1. Soveltamisala

1.1 Tämä politiikka perustaa organisaation henkilötietojen hallintajärjestelmän PII:n käsittelylle rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän yhteyksissä.

1.2 Tätä politiikkaa sovelletaan seuraaviin PIMS-alueisiin:

1.2.1 PIMS:n soveltamisala, toimintaympäristö, sidosryhmät ja organisatoriset rajat;

1.2.2 PIMS-roolin määrittäminen PII:n käsittelytoimille;

1.2.3 tietosuojapolitiikka, tietosuojatavoitteet, tietosuojariskien arviointi, tietosuojariskien käsittely ja PIMS:n soveltuvuuslausunto;

1.2.4 PIMS:n hallinnointi, seuranta, sisäinen tarkastus, johdon katselmointi, poikkeama, korjaavat toimenpiteet ja jatkuva parantaminen;

1.2.5 dokumentoitu tieto ja todentava aineisto, joita tarvitaan PIMS:n vaatimustenmukaisuuden ja osoitusvelvollisuuden osoittamiseen.

1.3 Tässä politiikassa olennainen muutos tarkoittaa muutosta, joka vaikuttaa PIMS:n soveltamisalaan, PII:n käsittelytarkoituksiin, PII-luokkiin, rekisteröityjen luokkiin, käsittelypaikkoihin, rekisterinpitäjän tai henkilötietojen käsittelijän roolien jakoon, järjestelmäarkkitehtuuriin, toimittaja- tai alikäsittelijäjärjestelyihin, tietosuojariskiprofiiliin, sovellettaviin lakisääteisiin tai sopimusperusteisiin velvoitteisiin taikka sertifioinnin soveltamisalaan.

2. Tarkoitus

2.1 Tämä politiikka määrittää pakolliset hallinnointivaatimukset PIMS:n perustamiselle, toteuttamiselle, ylläpitämiselle, seurannalle ja jatkuvalle parantamiselle.

2.2 Tämän politiikan tarkoituksena on varmistaa, että organisaatio voi osoittaa PII:n käsittelyn osoitusvelvollisen, riskiperusteisen ja näyttöön perustuvan hallinnan sovellettavissa PIMS-rooleissa.

3. Tavoitteet

3.1 Tämän politiikan tavoitteina on:

3.1.1 määrittää PIMS:n soveltamisala, toimintaympäristö, rajat ja roolien sovellettavuus;

3.1.2 osoittaa PIMS:n hallinnointivastuu käyttäen kanonisia PIMS-rooleja;

3.1.3 asettaa tietosuojatavoitteet ja mitattavat PIMS:n suorituskykyodotukset;

3.1.4 ylläpitää PIMS:n soveltuvuuslausuntoa valituista ja poissuljetuista kontrolleista;

3.1.5 integroida tietosuojariskien arviointi, tietosuojariskien käsittely ja DPIA-hallinnointi PIMS:n toimintaan;

3.1.6 varmistaa, että rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän velvoitteet tunnistetaan ennen käsittelyn aloittamista;

3.1.7 ylläpitää auditointivalmista todentavaa aineistoa valmiutta auditointia varten ja jatkuvaa parantamista varten;

3.1.8 välttää tarpeettomia rooleja, rekistereitä, lomakkeita ja päällekkäisiä operatiivisia kontrolleja.

4. Politiikkalausumat

4.1 PIMS:n perustaminen, toimintaympäristö ja soveltamisala

4.1.1 [Both] Top Management TULEE hyväksyä PIMS:n soveltamisala REG01:ssä ennen PIMS:n ensimmäistä toteutusta ja 30 päivän kuluessa olennaisesta muutoksesta.

4.1.2 [Both] Privacy Lead / PIMS Manager TULEE dokumentoida ulkoiset ja sisäiset tietosuojan toimintaympäristöön liittyvät seikat REG01:ssä vuosittain ja 30 päivän kuluessa olennaisesta muutoksesta.

4.1.3 [Both] Privacy Lead / PIMS Manager TULEE dokumentoida asiaankuuluvat sidosryhmät ja niiden PIMS-vaatimukset REG01:ssä vuosittain ja 30 päivän kuluessa olennaisesta muutoksesta.

4.1.4 [Both] Privacy Lead / PIMS Manager TULEE ylläpitää PIMS-prosessien vuorovaikutuksen yhteenvetoa REG01:ssä ennen jokaista johdon katselmointia.

4.2 PIMS-roolin määrittäminen

4.2.1 [Both] Process Owner / Business Owner TULEE luokitella organisaation PIMS-rooli kullekin PII:n käsittelytoimelle REG02:ssa ennen käsittelytoimen aloittamista.

4.2.2 [Joint Controller] Vendor / Procurement Owner TULEE dokumentoida yhteisrekisterinpitäjien vastuunjako REG08:ssa ennen yhteisen käsittelyn aloittamista.

4.2.3 [Processor] Vendor / Procurement Owner TULEE dokumentoida asiakkaan käsittelyohjeet henkilötietojen käsittelijän toimille REG08:ssa ennen palvelun käyttöönottoa.

4.2.4 [Subprocessor] Vendor / Procurement Owner TULEE dokumentoida ylemmän tason asiakkaan ohjeet ja hyväksytyt alikäsittelyjärjestelyt REG08:ssa ennen alikäsittelyn aloittamista.

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

9. Poikkeukset

9.1 Poikkeuspyyntö ja hyväksyntä

9.1.1 [All] Process Owner / Business Owner TULEE dokumentoida kaikki tätä politiikkaa koskevat poikkeuspyynnöt REG12:ssa ennen poikkeaman tapahtumista.

9.1.2 [Both] Privacy Lead / PIMS Manager TULEE arvioida kunkin pyydetyn poikkeuksen tietosuojariski REG04:ssä ennen hyväksyntää.

9.1.3 [Both] Top Management TULEE hyväksyä hyväksytyt tietosuojariskikynnykset ylittävät poikkeukset REG12:ssa ennen toteutusta.

9.1.4 [Both] Privacy Lead / PIMS Manager TULEE katselmoida aktiiviset PIMS-poikkeukset REG12:ssa neljännesvuosittain niiden sulkemiseen saakka.

9.2 Poikkeuksen sulkeminen

9.2.1 [All] Process Owner / Business Owner TULEE dokumentoida poikkeuksen sulkemista koskeva todentava aineisto REG12:ssa hyväksyttyyn poikkeuksen päättymispäivään mennessä.

9.2.2 [Both] Internal Audit / Compliance Reviewer TULEE todentaa vanhentuneiden poikkeusten sulkemista koskeva todentava aineisto REG12:ssa seuraavan suunnitellun sisäisen tarkastuksen aikana.

10. Soveltaminen

10.1 Poikkeamien käsittely

10.1.1 [All] Privacy Lead / PIMS Manager TULEE kirjata tätä politiikkaa koskevat epäillyt poikkeamat REG12:ssa viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [All] Process Owner / Business Owner TULEE toteuttaa hyväksytyt korjaavat toimenpiteet REG12:ssa niille asetettuun määräpäivään mennessä poikkeaman hyväksymisen jälkeen.

10.1.3 [All] Top Management TULEE katselmoida ratkaisemattomat merkittävät PIMS-poikkeamat REG12:ssa jokaisessa johdon katselmoinnissa.

10.1.4 [All] Internal Audit / Compliance Reviewer TULEE todentaa korjaavien toimenpiteiden vaikuttavuus REG12:ssa 30 päivän kuluessa ilmoitetusta sulkemisesta.

10.2 Eskalointi

10.2.1 [All] Privacy Lead / PIMS Manager TULEE eskaloida myöhässä olevat merkittävät korjaavat toimenpiteet roolille Top Management REG12:ssa viiden työpäivän kuluessa määräpäivän jälkeen.

10.2.2 [All] Top Management TULEE kirjata päätökset myöhässä olevista merkittävistä korjaavista toimenpiteistä REG12:ssa 15 työpäivän kuluessa eskaloinnista.

11. Katselmointi ja ylläpito

11.1 Politiikan katselmointi

11.1.1 [All] Privacy Lead / PIMS Manager TULEE katselmoida tämä politiikka REG12:ssa vuosittain ja 30 päivän kuluessa olennaisesta lakisääteisestä, organisatorisesta, käsittelyyn liittyvästä, teknologisesta tai sertifioinnin soveltamisalaan liittyvästä muutoksesta.

11.1.2 [All] Data Protection Officer / Privacy Advisor TULEE antaa dokumentoitua neuvontaa REG12:ssa ennen politiikan hyväksymistä, kun olennaiset tietosuojavelvoitteet muuttuvat.

11.1.3 [All] Top Management TULEE hyväksyä tähän politiikkaan tehtävät olennaiset muutokset REG12:ssa ennen julkaisemista.

11.1.4 [All] Privacy Lead / PIMS Manager TULEE päivittää REG01 ja REG03 15 työpäivän kuluessa hyväksytyistä politiikkamuutoksista, jotka muuttavat PIMS:n soveltamisalaa tai kontrollien sovellettavuutta.

11.1.5 [All] Privacy Lead / PIMS Manager TULEE kirjata hyväksytyistä politiikkamuutoksista viestiminen REG11:een 30 päivän kuluessa julkaisemisesta.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka

12.3 PII03 - PII:n käsittelyluettelon ja oikeusperusteen politiikka

12.4 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.5 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.6 PII12 - Henkilötietojen käsittelijöitä, alikäsittelijöitä ja tietojen jakamista koskeva politiikka

12.7 PII14 - PII:n turvallisuus- ja pääsynhallintapolitiikka

12.8 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.9 PII16 - Tietosuojakoulutus-, tietoisuus- ja pätevyyspolitiikka

12.10 PII17 - PIMS:n dokumentoidun tiedon ja todentavan aineiston hallintapolitiikka

12.11 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 4.1** - Kartoitettu organisaation toimintaympäristön, tietosuojan toimintaympäristöön liittyvien seikkojen sekä rekisterinpitäjän tai henkilötietojen käsittelijän roolin sovellettavuuden määrittämiseen PIMS-toimissa. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Kartoitettu sidosryhmien, rekisteröityjen, asiakkaiden, valvontaviranomaisten, henkilötietojen käsittelijöiden, alikäsittelijöiden ja niiden asiaankuuluvien PIMS-vaatimusten tunnistamiseen. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Kartoitettu dokumentoidun PIMS:n soveltamisalan määrittämiseen, hyväksymiseen, ylläpitoon ja muuttamiseen. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Kartoitettu PIMS-prosessien ja niiden vuorovaikutusten perustamiseen, toteuttamiseen, ylläpitoon ja parantamiseen. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Kartoitettu Top Managementin hyväksyntään, resursseihin, hallinnointikatselmointiin sekä johtajuuteen PIMS:n vaikuttavuuden ja parantamisen osalta. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Kartoitettu tämän tietosuojapolitiikan ylläpitämiseen hyväksyttynä dokumentoituna tietona ja politiikkamuutosten viestimiseen. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Kartoitettu PIMS-roolien, vastuiden ja valtuuksien osoittamiseen ja viestimiseen. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Kartoitettu PIMS:n riskejä ja mahdollisuuksia koskevien toimien suunnitteluun käyttäen toimintaympäristöä, sidosryhmien vaatimuksia, tavoitteita ja parantamissyötteitä. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Kartoitettu vaatimukseen tehdä tietosuojariskien arviointi ennen uutta tai olennaisesti muuttunutta käsittelyä ja ylläpitää tietosuojariskejä koskevaa todentavaa aineistoa. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Kartoitettu tietosuojariskien käsittelyyn, kontrollien valintaan, tietoturvaohjelman yhteyteen ja soveltuvuuslausunnon ylläpitoon. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Kartoitettu PIMS-tavoitteiden asettamiseen, mittaamiseen, seurantaan, viestimiseen ja päivittämiseen. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Kartoitettu suunniteltuihin PIMS-muutoksiin ja soveltamisalaan, rooleihin, kontrolleihin ja dokumentoituun tietoon vaikuttavien muutosten hallintaan. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Kartoitettu resurssien määrittämiseen ja tarjoamiseen PIMS:n perustamista, toimintaa, ylläpitoa ja parantamista varten. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Kartoitettu pätevyysodotuksiin ja PIMS-vastuita sekä roolisuoriutumista tukevaan todentavaan aineistoon. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Kartoitettu tietoisuuteen tietosuojapolitiikasta, panoksesta PIMS:n vaikuttavuuteen ja poikkeamien seurauksista. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Kartoitettu PIMS:n hallinnointiin, politiikkamuutoksiin ja eskalointiin liittyvään sisäiseen ja ulkoiseen viestintään. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Kartoitettu dokumentoidun tiedon laatimiseen, ylläpitoon, hallintaan, todentavan aineiston valmiuteen ja säilyttämiseen. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Kartoitettu PIMS:n operatiivisten prosessien ja ulkoisesti tuotettujen prosessien suunnitteluun, toteuttamiseen ja ohjaukseen. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Kartoitettu tietosuojariskien arviointien tekemiseen suunnitelluin väliajoin ja silloin, kun merkittäviä muutoksia ehdotetaan tai tapahtuu. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Kartoitettu tietosuojariskien käsittelysuunnitelmien toteuttamiseen ja käsittelyn tuloksia koskevan todentavan aineiston säilyttämiseen. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Kartoitettu seurantaan, mittaamiseen, analysointiin, arviointiin, mittareihin ja PIMS:n vaikuttavuuden raportointiin. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Kartoitettu sisäisen tarkastuksen suunnitteluun, todentavan aineiston otantaan, auditointituloksiin ja riippumattomaan katselmointiin. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Kartoitettu johdon katselmoinnin syötteisiin, suorituskyvyn katselmointiin, johdon katselmoinnin tuotoksiin ja parantamispäätöksiin. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Kartoitettu jatkuvaan parantamiseen johdon katselmoinnin, mittareiden, korjaavien toimenpiteiden seurannan ja politiikan ylläpidon avulla. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Kartoitettu poikkeamien käsittelyyn, korjaaviin toimenpiteisiin, eskalointiin, sulkemiseen ja vaikuttavuuden todentamiseen. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Kartoitettu rekisterinpitäjän puolen käsittelytarkoituksia koskeviin tallenteisiin, oikeusperusteen yhteyteen, DPIA-tarpeen määrittämiseen, yhteisrekisterinpitäjien vastuunjakoon ja käsittelyä koskeviin todentaviin tallenteisiin. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Kartoitettu henkilötietojen käsittelijän asiakassopimuksiin, dokumentoituihin asiakkaan ohjeisiin ja henkilötietojen käsittelijän tarkoitusrajoituksiin. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Kartoitettu PII:n turvallisuutta koskevan politiikan yhteyteen, PII:n tietoturvakontrollien perustason omistajuuteen ja tietoturvakontrollien tilaan PIMS:n soveltuvuuslausunnossa. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartoitettu osoitusvelvollisuutta koskevaan näyttöön, politiikan hyväksyntään, käsittelyroolin luokitukseen, kontrollien sovellettavuuteen, seurantaan, auditointiin ja korjaavien toimenpiteiden tallenteisiin. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän hallinnointitoimenpiteisiin, politiikan hyväksyntään, PIMS-tavoitteisiin, vaikuttavuuden katselmointiin ja rekisterinpitäjän osoitusvelvollisuutta koskevaan dokumentoituun näyttöön. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Kartoitettu yhteisrekisterinpitäjien vastuunjaon määrittämiseen ja dokumentointiin ennen yhteisen käsittelyn aloittamista. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Kartoitettu henkilötietojen käsittelijöiden ja alikäsittelijöiden hallinnointitallenteisiin, asiakkaan käsittelyohjeisiin ja ulkoisesti tuotettujen prosessien ohjaukseen. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Kartoitettu käsittelytoimien tallenteisiin, rooliluokitukseen, käsittelyn vastuullisuustallenteisiin ja auditoitavuutta varten säilytettävään todentavaan aineistoon. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Kartoitettu PII:n tietoturvaperustason hallinnointiin, tietoturvakontrollien omistajuuteen, tietoturvan toteutuksen tilaan ja operatiivisten kontrollien vahvistamiseen. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Kartoitettu DPIA-tarpeen määrittämiseen ja tietosuojariskien arviointiin ennen kuin korkean riskin tai olennaisesti muuttunut rekisterinpitäjän käsittely etenee. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Kartoitettu tietosuojakontrollien tunnistamiseen, tietosuojaperiaatteisiin, tietoturvaan, tietosuojavaatimusten noudattamiseen, auditointiin, todentavaan aineistoon ja riskiperusteiseen tietosuojan hallinnointiin. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Kartoitettu PIA-hallinnointiin, DPIA-laukaisijan määrittämiseen, PIA-valmisteluun, tietosuojariskikriteereihin ja dokumentoituun tietosuojariskien arvioinnin näyttöön. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Kartoitettu PII:n suojausohjelman vaatimuksiin, PII:n suojausvaatimusten tunnistamiseen, tietosuojariskiperusteiseen kontrollien valintaan ja PII:n suojauspolitiikan ohjaukseen. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Kartoitettu organisaation tietosuojariskien periaatteisiin, johdon sitoutumiseen, tietosuojariskien integrointiin PIMS:n hallinnointiin ja organisaation roolin ymmärtämiseen PII:n käsittelyssä. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].