					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII02					Asiakirjan nimi: **Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden 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	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	PIMS-roolin konteksti
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Johtajuus ja osoitusvelvollisuus
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS-roolit, vastuut ja toimivaltuudet
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Roolikohtainen pätevyys
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Roolikohtainen tietoisuus
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Rooleja koskeva viestintä
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Rooleja koskeva dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operatiivisten kontrollien omistajuus
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Riippumaton auditointirooli
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Osoitusvelvollisuuden johdon katselmointi
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Rooleihin liittyvä poikkeama ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Henkilötietojen käsittelijän sopimusvastuu
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Yhteisrekisterinpitäjien roolit ja vastuut
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Osoitusvelvollisuuden dokumentaatio
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Henkilötietojen käsittelijän asiakassopimukset ja ohjeet
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Henkilötietojen käsittelijän tarkoituksen yhdenmukaisuus
GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuutta tukeva todentava aineisto

GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän vastuu ja toimenpiteet
GDPR	Article 26	Joint Controller	Supporting	Yhteisrekisterinpitäjien järjestelyt
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijöiden hallinnointi ja ohjeet
GDPR	Article 30	Both	Supporting	Käsittelytoimien tallenteet ja vastuuta osoittava todentava aineisto
GDPR	Article 37	Conditional	Referenced	Tietosuojavastaavan nimeäminen soveltuvissa tilanteissa
GDPR	Article 38	Conditional	Supporting	Tietosuojavastaavan asema ja riippumattomuus soveltuvissa tilanteissa
GDPR	Article 39	Conditional	Supporting	Tietosuojavastaavan tehtävät soveltuvissa tilanteissa
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Tietosuoja- ja yksityisyydensuojan viitekehyksen toimijat ja roolit
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Tietosuojan vaatimustenmukaisuuden osoitusvelvollisuus
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	PII-suojauksen roolit ja tehtävien eriyttäminen
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Tietoturvaroolit ja -vastuut
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Tehtävien eriyttäminen

1. Soveltamisala

1.1 Tämä politiikka määrittää PIMS-roolimallin, osoitusvelvollisuuden rakenteen, vastuiden osoittamista koskevat säännöt, roolien yhdistämistä koskevat säännöt, eskalointiodotukset ja todentavaa aineistoa koskevat vaatimukset tietosuojan hallinnointia varten.

1.2 Tätä politiikkaa sovelletaan henkilöstöön, toimintoihin, järjestelmiin, toimittajiin, henkilötietojen käsittelijöihin, alikäsittelijöihin ja yhteisrekisterinpitäjäsuhteisiin, jotka osallistuvat PII-käsittelyyn tai vaikuttavat siihen PIMS-soveltamisalan piirissä.

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

1.4 Tämä politiikka ei luo uusia organisaation tehtävänimikkeitä. Se määrittää kanoniset PIMS-roolit, jotka voidaan osoittaa nykyisille henkilöille tai toiminnoille edellyttäen, että roolin osoittaminen, pätevyys, riippumattomuus ja eturistiriitoja koskevat vaatimukset dokumentoidaan.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että PIMS-vastuut osoitetaan selkeästi, ymmärretään, viestitään, todennetaan todentavalla aineistolla, katselmoidaan ja niitä parannetaan.

2.2 Tämä politiikka mahdollistaa sen, että organisaatio voi osoittaa vastuunsa tietosuojan hallinnoinnista, PII-käsittelyn omistajuudesta, rekisterinpitäjän ja henkilötietojen käsittelijän roolin määrittämisestä, yhteisrekisterinpitäjien vastuunjaosta, henkilötietojen käsittelijän ohjeiden käsittelystä, toimittajien tietosuojavastuista, riippumattomasta arvioinnista ja roolipohjaisesta eskaloinnista.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää kanoniset PIMS-roolit, joita käytetään koko PIMS-politiikkakokonaisuudessa;

3.1.2 varmistaa, että jokaiselle olennaiselle PIMS-vastuulle on osoitettu vastuullinen rooli;

3.1.3 tukea rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän osoitusvelvollisuutta;

3.1.4 sallia roolien käytännöllinen yhdistäminen pienissä ja keskisuurissa organisaatioissa samalla, kun eturistiriitoja hallitaan;

3.1.5 säilyttää Internal Audit / Compliance Reviewer -roolin riippumaton arviointi;

3.1.6 varmistaa, että roolien osoittaminen ja roolimuutokset kirjataan kanonisiin todentavan aineiston kohteisiin;

3.1.7 varmistaa, että PIMS-roolin haltijat saavat asianmukaista viestintää ja tietoisuutta;

3.1.8 varmistaa, että rooleihin liittyvät puutteet, ristiriidat ja poikkeamat eskaloidaan ja korjataan.

4. Politiikkalausumat

4.1 PIMS-roolimalli ja roolien osoittaminen

4.1.1 [All] Top Management MUST hyväksyä kanoninen PIMS-roolimalli rekisterissä REG01 ennen PIMS:n ensimmäistä käyttöönottoa ja sen jälkeen vuosittain.

4.1.2 [All] Privacy Lead / PIMS Manager MUST ylläpitää nimettyjä PIMS-roolien osoituksia rekisterissä REG01 ennen PIMS:n käyttöönottoa ja 10 työpäivän kuluessa henkilöstö- tai organisaatiomuutoksista.

4.1.3 [All] Privacy Lead / PIMS Manager MUST dokumentoida kunkin osoitetun PIMS-roolin vastuualue ja toimivaltataso rekisterissä REG01 ennen kuin osoitus tulee voimaan.

4.1.4 [All] Process Owner / Business Owner MUST osoittaa vastuullinen käsittelynomistaja jokaiselle PII-käsittelytoimelle rekisterissä REG02 ennen käsittelytoimen aloittamista.

4.1.5 [All] System Owner / Application Owner MUST dokumentoida vastuullinen järjestelmäomistaja jokaiselle PII:tä käsittelevälle järjestelmälle rekisterissä REG02 ennen järjestelmän tuotantokäyttöönottoa.

4.1.6 [All] Vendor / Procurement Owner MUST dokumentoida suhteen omistaja jokaiselle henkilötietojen käsittelijälle, alikäsittelijälle, kolmannen osapuolen tietojen jakamiselle tai yhteisrekisterinpitäjäsuhteelle rekisterissä REG08 ennen käyttöönottoa tai sopimuksen hyväksymistä.

4.2 Roolien yhdistäminen, eriyttäminen ja riippumattomuus

4.2.1 [All] Privacy Lead / PIMS Manager MUST dokumentoida jokainen PIMS-roolien yhdistäminen rekisterissä REG01 ennen kuin roolien yhdistäminen tulee voimaan.

4.2.2 [All] Top Management MUST hyväksyä roolien yhdistämiset, jotka koskevat rooleja Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator tai Internal Audit / Compliance Reviewer, rekisterissä REG01 ennen osoittamista.

4.2.3 [All] Internal Audit / Compliance Reviewer MUST dokumentoida riippumattomuus katselmoitavasta PIMS-prosessista rekisterissä REG12 ennen jokaisen PIMS-auditoinnin tai vaatimustenmukaisuuden katselmoinnin aloittamista.

4.2.4 [All] Privacy Lead / PIMS Manager MUST kirjata korvaavat kontrollit väistämättömille eriyttämisristiriidoille rekisterissä REG12 ennen roolien yhdistämisen hyväksymistä.

4.2.5 [All] Data Protection Officer / Privacy Advisor MUST kirjata roolin riippumattomuutta koskevat huolenaiheet tai eturistiriitoja koskevat huolenaiheet rekisterissä REG12 viiden työpäivän kuluessa niiden tunnistamisesta.

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

9. Poikkeukset

9.1.1 [All] Process Owner / Business Owner MUST pyytää roolin osoitusvelvollisuutta koskevaa poikkeusta rekisterissä REG12 ennen PII-käsittelytoimen toteuttamista ilman vaadittua osoitettua roolia.

9.1.2 [All] Privacy Lead / PIMS Manager MUST arvioida kunkin roolin osoitusvelvollisuutta koskevan poikkeuksen vaikutus ja lieventämistoimet rekisterissä REG12 10 työpäivän kuluessa pyynnöstä.

9.1.3 [All] Top Management MUST hyväksyä roolin osoitusvelvollisuutta koskevat poikkeukset, jotka ylittävät 30 päivää tai vaikuttavat korkean riskin käsittelyyn, rekisterissä REG12 ennen kuin poikkeus tulee voimaan.

9.1.4 [All] Privacy Lead / PIMS Manager MUST asettaa kullekin hyväksytylle roolin osoitusvelvollisuutta koskevalle poikkeukselle enintään 90 päivän päättymispäivä rekisterissä REG12 ennen hyväksyntää.

9.1.5 [All] Privacy Lead / PIMS Manager MUST sulkea tai arvioida uudelleen jokainen roolin osoitusvelvollisuutta koskeva poikkeus rekisterissä REG12 viiden työpäivän kuluessa päättymisestä.

10. Soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager MUST kirjata puuttuvat, virheelliset tai vanhentuneet PIMS-roolien osoitukset poikkeamina rekisterissä REG12 viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [All] Top Management MUST edellyttää korjaavia toimenpiteitä rekisterissä REG12 15 työpäivän kuluessa toistuvista tai pitkittyneistä osoitusvelvollisuuden epäonnistumisista.

10.1.3 [All] Process Owner / Business Owner MUST estää uuden tai muutetun PII-käsittelyn tuotantokäyttöönotto, jos vaadittu roolia ja osoitusvelvollisuutta koskeva todentava aineisto puuttuu rekisteristä REG02 tai REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer MUST varmentaa roolin osoitusvelvollisuutta koskevien poikkeamien korjaavien toimenpiteiden vaikuttavuus rekisterissä REG12 seuraavassa aikataulutetussa auditoinnissa tai 60 päivän kuluessa sulkemisesta sen mukaan, kumpi tapahtuu ensin.

11. Katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager MUST katselmoida tämä politiikka vuosittain ja 30 päivän kuluessa PIMS-roolimallin olennaisesta muutoksesta.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUST katselmoida tähän politiikkaan ehdotetut muutokset tietosuojaroolien vaikutusten osalta rekisterissä REG12 ennen hyväksyntää.

11.1.3 [All] Top Management MUST hyväksyä tähän politiikkaan tehtävät olennaiset muutokset rekisterissä REG12 ennen julkaisemista.

11.1.4 [All] Privacy Lead / PIMS Manager MUST päivittää REG01 ja REG11 15 työpäivän kuluessa PIMS-rooleihin, vastuisiin tai viestintävaatimuksiin hyväksytyistä muutoksista.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.3 PII03 - PII-käsittelyinventaarion ja oikeusperusteen politiikka

12.4 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.5 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.6 PII12 - Henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojan hallintapolitiikka

12.7 PII14 - PII-turvallisuuden ja pääsynhallinnan politiikka

12.8 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.9 PII16 - Tietosuojakoulutus-, tietoisuus- ja pätevyyspolitiikka

12.10 PII17 - PIMS-dokumentoidun tiedon ja todentavan aineiston hallintapolitiikka

12.11 PII18 - PIMS-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 yksilöi sisäiset lausekkeet, joilla ne toteutetaan tai joita ne tukevat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Kartoitettu PIMS-roolikontekstin määrittämiseen, rekisterinpitäjän ja henkilötietojen käsittelijän sovellettavuuteen, käsittelyn omistajuuteen ja suhteiden vastuukirjauksiin. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Kartoitettu roolin Top Management hyväksyntään, osoitusvelvollisuuden valvontaan, vuosittaiseen johdon katselmointiin, osoitusvelvollisuutta koskeviin mittareihin ja roolien epäonnistumisia koskeviin korjaaviin toimenpiteisiin. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Kartoitettu PIMS-roolien, vastuiden ja toimivaltuuksien osoittamiseen, dokumentointiin, viestintään ja ylläpitoon sekä järjestelmäomistajuuteen, käsittelyn omistajuuteen, toimittajasuhteiden omistajuuteen, poikkeamaeskaloinnin omistajuuteen ja

riippumattoman arvioinnin vastuuseen. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Kartoitettu roolikohtaista pätevyyttä ja tietoisuutta koskevaan todentavaan aineistoon osoitettujen PIMS-vastuiden osalta. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Kartoitettu osoitettujen PIMS-vastuiden tietoisuuteen, hyväksyntää koskevaan todentavaan aineistoon ja vuosittaiseen roolitietoisuuden raportointiin. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Kartoitettu roolien osoittamisen, roolimuutosten, eskalointien ja roolin luovutustietojen viestintään. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Kartoitettu PIMS-roolien osoittamista, vastuualueita, toimivaltatasoja, vuosittaista todentavan aineiston säilyttämistä ja roolimatriisin ylläpitoa koskevaan dokumentoituun tietoon. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Kartoitettu käsittelytoimien, järjestelmien, toimittajien, henkilötietojen käsittelijöiden, alikäsittelijöiden, yhteisrekisterinpitäjäsuhteiden ja tuotantokäyttöönoton kontrollien operatiiviseen kontrolliomistajuuteen. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Kartoitettu roolien osoittamista koskevan todentavan aineiston, roolien yhdistämistä koskevan todentavan aineiston, riippumattomuutta koskevan todentavan aineiston, havaintojen ja korjaavien toimenpiteiden sulkemisen riippumattomaan auditointiin ja vaatimustenmukaisuuden katselmointiin. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Kartoitettu PIMS-roolien osoittamisen kattavuuden, rooliristiriitojen, poikkeusten, osoitusvelvollisuusmittareiden ja osoitusvelvollisuuskatselmoinnin tulosten johdon katselmointiin. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Kartoitettu roolien osoitusvelvollisuuteen liittyvien asioiden eskalointiin, poikkeamien kirjaamiseen, korjaaviin toimenpiteisiin, poikkeusten sulkemiseen ja vaikuttavuuden varmentamiseen. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Kartoitettu henkilötietojen käsittelijän sopimusvastuun ja kolmannen osapuolen vastuun eskaloinnin osoittamiseen ja dokumentointiin ennen sopimuksen hyväksymistä tai uusimista. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Kartoitettu yhteisrekisterinpitäjien vastuunjaon ja suhteiden vastuuta koskevan todentavan aineiston dokumentointiin ennen yhteisrekisterinpitäjien käsittelyn aloittamista. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Kartoitettu rekisterinpitäjän käsittelyn omistajuutta, rooliluokittelua ja todentavan aineiston omistajuutta koskevan osoitusvelvollisuuden dokumentaation ylläpitoon. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Kartoitettu henkilötietojen käsittelijän asiakassopimusvastuuseen, asiakkaan ohjeiden omistajuuteen ja henkilötietojen käsittelijäsuhdetta koskevaan todentavaan aineistoon. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Kartoitettu henkilötietojen käsittelijän tarkoituksen ja ohjeiden yhdenmukaisuuteen asiakkaan ohjeiden omistajuuden sekä rekisterinpitäjän ja henkilötietojen käsittelijän roolin varmentamisen kautta. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartoitettu osoitusvelvollisuutta koskevaan todentavaan aineistoon roolien osoittamisesta, käsittelyn omistajuudesta, roolikatselmoinneista, poikkeamista ja auditointihavainnoista. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän vastuuseen, vastuulliseen käsittelyn omistajuuteen, roolin Top Management valvontaan, vuosittaiseen katselmointiin ja osoitusvelvollisuustoimenpiteisiin. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Kartoitettu yhteisrekisterinpitäjien vastuunjaon ja suhteiden vastuuta koskevan todentavan aineiston dokumentointiin ennen yhteisrekisterinpitäjien käsittelyn aloittamista. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Kartoitettu henkilötietojen käsittelijän ja alikäsittelijän vastuunjakoon, asiakkaan ohjeiden omistajuuteen, sopimusvastuuseen ja kolmansien osapuolten eskalointipolkuihin. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Kartoitettu käsittelytoimia koskeviin tallenteisiin, käsittelyn omistajuuteen, PIMS-rooliluokitteluun ja rekisterinpitäjän tai henkilötietojen käsittelijän roolin varmentamiseen. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Kartoitettu Data Protection Officer / Privacy Advisor -roolin dokumentointiin, kun nimeäminen on sovellettavaa tai rooli on osoitettu vapaaehtoisesti. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Kartoitettu Data Protection Officer / Privacy Advisor -roolin asemaan, riippumattomuuteen, osallistamiseen ja eturistiriitojen käsittelyyn soveltuvissa tilanteissa. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Kartoitettu Data Protection Officer / Privacy Advisor -roolin tietosuojaa koskevaan neuvontaan, seurannassa tehtyihin huomioihin, neuvonnalliseen katselmointiin ja rooleihin liittyvien tietosuojavaikutusten katselmointiin soveltuvissa tilanteissa. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Kartoitettu tietosuoja- ja yksityisyydensuojan viitekehyksen toimijoihin ja roolien jakamiseen rekisteröidyille, PII-rekisterinpitäjille, PII-käsittelijöille, kolmansille osapuolille ja PIMS-rooliluokittelulle. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Kartoitettu tietosuojan vaatimustenmukaisuuden osoitusvelvollisuuteen, roolia koskevaan todentavaan aineistoon, katselmointiin, auditointihavaintoihin ja korjaavien toimenpiteiden vaikuttavuuden varmentamiseen. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Kartoitettu PII-suojauksen roolien määrittelyyn, roolien dokumentointiin, rooleja koskevaan viestintään, tietoturvan ja tietosuojan koordinointiin sekä PII-suojauksen tehtävien eriyttämiseen. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Kartoitettu PIMS- ja tietoturvavastuiden määrittämiseen, osoittamiseen, dokumentointiin, viestintään ja ylläpitoon. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Kartoitettu tehtävien eriyttämiseen, roolien yhdistämisen hyväksyntään, riippumattomaan arviointiin, ristiriitojen hallintakeinoihin ja rooliristiriitojen korjaavien

toimenpiteiden vaikuttavuuden varmentamiseen. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].