					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII18					Asiakirjan nimi: **PIMS-seurannan, auditoinnin ja parantamisen 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 6.2	Both	Supporting	Tietosuojatavoitteiden mittaaminen
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Seurantaa, auditointia ja parantamista koskeva dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operatiivisen suunnittelun ja ohjauksen seuranta
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Seuranta, mittaaminen, analysointi ja arviointi
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Sisäinen auditointi
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.1.2.9	Controller	Supporting	Auditoinnissa käytettävät rekisterinpitäjän käsittelytallenteet
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Henkilötietojen käsittelijän sopimusta ja auditointiyhteistyötä koskeva todentava aineisto
GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuuden todentava aineisto
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän toimenpiteet ja vaikuttavuuden katselmointi
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijän auditoinnin ja yhteistyön hallinnointi
GDPR	Article 30	Both	Supporting	Auditoinnissa käytettävät käsittelytallenteet
GDPR	Article 32	Both	Supporting	Turvallisuustoimenpiteiden testaaminen ja arviointi
GDPR	Article 39	Conditional	Supporting	DPO:n seuranta ja auditointia koskeva neuvonta soveltuvin osin
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Tietosuojan vaatimustenmukaisuus, auditointi ja riippumaton valvonta

ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Henkilötietojen suojauksen katselmointi ja vaatimustenmukaisuustarkastukset
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Tietoturvallisuuden seuranta ja arviointi
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS:n sisäisen auditoinnin tuki
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS:n johdon katselmoinnin tuki
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS:n jatkuvan parantamisen tuki
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS:n poikkeamien ja korjaavien toimenpiteiden tuki
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Tietoturvallisuuden riippumaton katselmointi
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Politiikkojen ja standardien vaatimustenmukaisuuden katselmointi
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Hallintajärjestelmäauditoinnin periaatteet, ohjelma, toteutus ja pätevyys

1. Soveltamisala

1.1 Tässä politiikassa määritellään organisaation vaatimukset PIMS-seurannalle, mittaamiselle, analysoinnille, arvioinnille, sisäiselle auditoinnille, johdon katselmoinnille, poikkeamien käsittelylle, korjaaville toimenpiteille ja jatkuvalle parantamiselle.

1.2 Tätä politiikkaa sovelletaan seuraaviin:

1.2.1 kaikki PIMS-prosessit, kontrollit, politiikat, rekisterit, näyttöobjektit, järjestelmät, toimittajat, henkilötietojen käsittelijät, alikäsittelijät ja tietojen jakamista koskevat järjestelyt PIMS:n soveltamisalassa;

1.2.2 organisaation rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän kontekstit;

1.2.3 PIMS-suorituskyvyn, tietosuojatavoitteiden, kontrollien toteutuksen tilan, auditointihavaintojen, poikkeamien, korjaavien toimenpiteiden, johdon katselmoinnin toimenpiteiden ja parantamistoimien koottu seuranta;

1.2.4 REG12:ssa säilytettävä todentava aineisto sekä REG01–REG11:ssä säilytettävä sitä tukeva lähdeaineisto.

1.3 Tämä politiikka ei korvaa muissa PIMS-politiikoissa määriteltyjä operatiivisen seurannan vaatimuksia. Se määrittää PIMS:n kootun suorituskyvyn arvioinnin, auditoinnin, katselmoinnin ja parantamisen syklin.

1.4 Tässä politiikassa merkittävä PIMS-poikkeama tarkoittaa epäonnistumista, joka vaikuttaa olennaisesti PIMS:n soveltamisalaan, tietosuojatavoitteisiin, henkilötietojen käsittelyn osoitusvelvollisuuteen, tietosuojariskien käsittelyyn, rekisteröityjen oikeuksiin, käsittelyn turvallisuuteen, henkilötietojen käsittelijän tai alikäsittelijän hallinnointiin, henkilötietojen tietoturvaloukkausvalmiuteen, dokumentoidun todentavan aineiston eheyteen, sertifioinnin soveltamisalaan tai saman vaatimuksen toistuvaan epäonnistumiseen 12 kuukauden aikana.

1.5 Tässä politiikassa olennainen muutos tarkoittaa mitä tahansa muutosta, joka vaikuttaa PIMS:n soveltamisalaan, henkilötietojen käsittelyn tarkoituksiin, henkilötietoryhmiin, rekisteröityjen ryhmiin, käsittelypaikkoihin, rekisterinpitäjän tai henkilötietojen käsittelijän roolien kohdentamiseen, järjestelmäarkkitehtuuriin, toimittaja- tai alikäsittelijäjärjestelyihin, tietosuojariskiprofiiliin, sovellettaviin lakisääteisiin tai sopimusperusteisiin velvoitteisiin, auditoinnin soveltamisalaan, seurantamenetelmään tai sertifioinnin soveltamisalaan.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että organisaatio arvioi PIMS:n suorituskykyä, todentaa PIMS:n vaatimustenmukaisuuden, tunnistaa poikkeamat, korjaa kontrollien heikkoudet ja parantaa PIMS:ää jatkuvasti objektiivisen todentavan aineiston perusteella.

2.2 Tämä politiikka mahdollistaa sen osoittamisen, että PIMS:n seuranta-, auditointi-, johdon katselmointi- ja parantamistoimet ovat suunniteltuja, tarvittaessa riippumattomia, näyttöön perustuvia, oikea-aikaisia ja jäljitettävissä vastuullisiin rooleihin ja kanonisiin näyttöobjekteihin.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää koottu PIMS-seuranta- ja mittausprosessi;

3.1.2 varmistaa, että tietosuojatavoitteita ja PIMS-kontrollien suorituskykyä mitataan dokumentoidun todentavan aineiston avulla;

3.1.3 perustaa riskiperusteinen sisäisen auditoinnin ohjelma PIMS:lle;

3.1.4 säilyttää riippumattomuus ja objektiivisuus PIMS-auditointitoiminnoissa;

3.1.5 varmistaa, että johdon katselmointi saa täydelliset ja ajantasaiset PIMS:n suorituskykyä koskevat lähtötiedot;

3.1.6 varmistaa, että poikkeamat kirjataan, arvioidaan, korjataan ja varmennetaan;

3.1.7 varmistaa, että korjaavia toimenpiteitä seurataan sulkemiseen asti ja niiden vaikuttavuus katselmoidaan;

3.1.8 tunnistaa toistuvat heikkoudet ja parantamismahdollisuudet;

3.1.9 tukea valmiutta auditointia varten ja vastuutettua todentavan aineiston hallintaa;

3.1.10 välttää muissa PIMS-politiikoissa jo määriteltyjen operatiivisten mittareiden päällekkäisyys.

4. Politiikkalausekkeet

4.1 PIMS-seurannan ja mittaamisen viitekehys

4.1.1 [Both] Privacy Lead / PIMS Manager MUST määrittää koottu PIMS-seurantaohjelma REG12:ssa ennen PIMS:n ensimmäistä käyttöönottoa ja sen jälkeen vuosittain.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST määrittää kunkin PIMS-mittarin mittausmenetelmä, mittaustiheys, todentavan aineiston lähde, tavoite ja vastuullinen rooli REG12:ssa ennen mittaussyklin alkamista.

4.1.3 [Both] Process Owner / Business Owner MUST toimittaa henkilötietojen käsittelytoimien seurannan lähtötiedot REG02:sta roolille Privacy Lead / PIMS Manager neljännesvuosittain.

4.1.4 [Both] Information Security Lead MUST toimittaa henkilötietojen tietoturvakontrollien tilaa koskevat lähtötiedot REG03:sta roolille Privacy Lead / PIMS Manager neljännesvuosittain.

4.1.5 [Both] Vendor / Procurement Owner MUST toimittaa henkilötietojen käsittelijöiden, alikäsittelijöiden, kolmansien osapuolten kanssa tapahtuvan jakamisen ja toimittajavarmennuksen tilaa koskevat lähtötiedot REG08:sta roolille Privacy Lead / PIMS Manager neljännesvuosittain.

4.1.6 [All] Incident Response Coordinator MUST toimittaa henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten trenditiedot REG10:stä roolille Privacy Lead / PIMS Manager kuukausittain ja 10 työpäivän kuluessa merkittävän poikkeaman sulkemisesta.

4.1.7 [Both] Privacy Lead / PIMS Manager MUST koota PIMS-seurannan tulokset REG12:een neljännesvuosittain.

4.2 PIMS:n sisäisen auditoinnin ohjelma

4.2.1 [All] Internal Audit / Compliance Reviewer MUST laatia riskiperusteinen PIMS:n sisäisen auditoinnin ohjelma REG12:een vuosittain ennen ensimmäistä suunniteltua PIMS-auditointisykliä.

4.2.2 [All] Internal Audit / Compliance Reviewer MUST määrittää kunkin PIMS-auditoinnin tavoite, kriteerit, soveltamisala, menetelmä, otantaperuste ja raportoinnin määräaika REG12:ssa ennen auditoinnin kenttätyön aloittamista.

4.2.3 [All] Internal Audit / Compliance Reviewer MUST kirjata auditoijan riippumattomuuden ja eturistiriitojen tarkastukset REG12:een ennen kutakin auditointitehtävää.

4.2.4 [All] Privacy Lead / PIMS Manager MUST asettaa pyydetyn valvotun PIMS:n dokumentoidun tiedon ja rekistereihin perustuvan todentavan aineiston saataville REG12:n kautta 10 työpäivän kuluessa hyväksytystä auditointipyynnöstä.

4.2.5 [Both] Internal Audit / Compliance Reviewer MUST testata sovellettavien PIMS-kontrollien toteutuksen tila REG03:a vasten kunkin PIMS-auditoinnin aikana.

4.2.6 [Both] Internal Audit / Compliance Reviewer MUST kirjata valittu henkilötietojen käsittelyä koskeva todentavan aineiston otos REG12:een kunkin PIMS-auditoinnin aikana.

4.2.7 [All] Internal Audit / Compliance Reviewer MUST kirjata PIMS-auditoinnin tulokset REG12:een 15 työpäivän kuluessa auditoinnin valmistumisesta.

4.2.8 [All] Privacy Lead / PIMS Manager MUST nimetä korjaavien toimenpiteiden omistajat hyväksytyille PIMS-auditointihavainnoille REG12:ssa 10 työpäivän kuluessa auditointitulosten hyväksymisestä.

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

9. Poikkeukset

9.1 Seurantaa, auditointia ja parantamista koskevat poikkeukset

9.1.1 [All] Process Owner / Business Owner MUST pyytää kaikki tätä politiikkaa koskevat poikkeukset REG12:ssa ennen poikkeaman tapahtumista.

9.1.2 [All] Privacy Lead / PIMS Manager MUST arvioida kunkin pyydetyn poikkeuksen vaikutus tietosuojaan, sertifiointiin, auditointiin ja korjaaviin toimenpiteisiin REG12:ssa 10 työpäivän kuluessa pyynnöstä.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST kirjata neuvonta REG12:een ennen sellaisen poikkeuksen hyväksymistä, joka vaikuttaa lakisääteisiin velvoitteisiin, rekisteröityjen oikeuksiin, DPIA-sitoumuksiin, asiakkaan auditointivelvoitteisiin tai korkean riskin käsittelyyn.

9.1.4 [All] Top Management MUST hyväksyä auditointiaikataulun valmistumiseen, johdon katselmointiin, merkittäviin poikkeamiin, sertifioinnin soveltamisalaan tai korkean riskin käsittelyyn vaikuttavat poikkeukset REG12:ssa ennen poikkeuksen voimaantuloa.

9.1.5 [All] Privacy Lead / PIMS Manager MUST asettaa kullekin hyväksytylle seuranta-, auditointi- tai parantamispoikkeukselle enintään 90 päivän päättymispäivä REG12:ssa.

9.1.6 [All] Privacy Lead / PIMS Manager MUST sulkea tai arvioida uudelleen kukin seuranta-, auditointi- tai parantamispoikkeus REG12:ssa viiden työpäivän kuluessa päättymisestä.

10. Soveltaminen

10.1 Seuranta-, auditointi- ja parantamisvaatimusten soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager MUST kirjata toteutumaton seurantasykli, toteutumaton PIMS-auditointi, viivästynyt johdon katselmointi, puuttuva auditointinäyttö, viivästynyt korjaava toimenpide tai viivästynyt parantamistoimi poikkeamana REG12:een viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [All] Internal Audit / Compliance Reviewer MUST kirjata auditointihavainnon vakavuus REG12:een ennen auditointiraportin julkaisemista.

10.1.3 [All] Top Management MUST edellyttää korjaavia toimenpiteitä kullekin merkittävälle PIMS-poikkeamalle REG12:ssa 10 työpäivän kuluessa eskaloinnista.

10.1.4 [All] Process Owner / Business Owner MUST estää tuotantokäyttöönotto tai ulkoisen varmentamisen toimittaminen korkean riskin käsittelylle, jos vaadittu korjaavien toimenpiteiden todentava aineisto puuttuu REG12:sta ennen tuotantokäyttöönottoa tai toimittamista.

10.1.5 [All] Privacy Lead / PIMS Manager MUST eskaloida toistuvat toteutumattomat seurannan tai korjaavien toimenpiteiden määräajat roolille Top Management REG12:ssa viiden työpäivän kuluessa toisesta esiintymästä 12 kuukauden aikana.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST varmentaa soveltamistoimen sulkeminen REG12:ssa seuraavassa aikataulutetussa auditoinnissa tai 60 päivän kuluessa ilmoitetusta sulkemisesta sen mukaan, kumpi tapahtuu ensin.

11. Katselmointi ja ylläpito

11.1 Politiikan katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager MUST katselmoida tämä politiikka REG12:ssa vuosittain ja 30 päivän kuluessa PIMS-seurantaa, auditointia, johdon katselmointia, korjaavia toimenpiteitä tai sertifiointia koskevien vaatimusten olennaisesta muutoksesta.

11.1.2 [All] Internal Audit / Compliance Reviewer MUST katselmoida PIMS-auditointiohjelman vaikuttavuus REG12:ssa vuosittain PIMS-toimintavuoden viimeisen aikataulutetun auditoinnin jälkeen.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST katselmoida tämän politiikan tietosuojan kannalta merkittävät muutokset REG12:ssa ennen hyväksymistä.

11.1.4 [All] Top Management MUST hyväksyä tämän politiikan olennaiset muutokset REG12:ssa ennen julkaisemista.

11.1.5 [All] Privacy Lead / PIMS Manager MUST päivittää REG01 ja REG03 15 työpäivän kuluessa tähän politiikkaan hyväksytyistä muutoksista, jotka muuttavat PIMS:n soveltamisalaa tai kontrollien sovellettavuutta.

11.1.6 [All] Privacy Lead / PIMS Manager MUST kirjata tätä politiikkaa koskevien hyväksyttyjen muutosten viestintä REG11:een 30 päivän kuluessa julkaisemisesta.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.3 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka

12.4 PII03 - Henkilötietojen käsittelyluettelon ja oikeusperusteen politiikka

12.5 PII04 - Tietosuojaselosteen ja läpinäkyvyyden politiikka

12.6 PII05 - Suostumuksen ja valinta-asetusten hallinnan politiikka

12.7 PII06 - Rekisteröityjen 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, luovuttamisen ja jakamisen politiikka

12.11 PII10 - Henkilötietojen säilytyksen, poistamisen ja hävittämisen politiikka

12.12 PII11 - Henkilötietojen täsmällisyyden ja laadun politiikka

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

12.14 PII13 - Henkilötietojen kansainvälisen siirron politiikka

12.15 PII14 - Henkilötietojen tietoturvan ja pääsynhallinnan politiikka

12.16 PII15 - Henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallintapolitiikka

12.17 PII16 - Tietosuojakoulutuksen, tietoisuuden ja pätevyyden politiikka

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

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 6.2** - Kartoitettu PIMS-tavoitteiden ja PIMS:n suorituskykymittareiden määrittämiseen, mittaamiseen, raportointiin ja katselmointiin. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Kartoitettu dokumentoidun tiedon ylläpitoon seurantatuloksista, auditointiohjelmista, auditointituloksista, johdon katselmoinnin todentavasta aineistosta, poikkeamista, korjaavista toimenpiteistä ja parantamistoimista. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Kartoitettu suunnitellun PIMS-seuranta-, auditointi-, korjaavien toimenpiteiden ja parantamissyklin käyttöön osana PIMS:n operatiivista ohjausta. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Kartoitettu seurannan ja mittaamisen kohteiden määrittämiseen, seurantatulosten kokoamiseen, PIMS:n suorituskyvyn arviointiin ja mittausnäytön ylläpitoon. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Kartoitettu sisäisen auditoinnin ohjelman ylläpitoon, auditoinnin suunnitteluun, auditoijan riippumattomuuden tarkastuksiin, todentavan aineiston otantaan, auditointituloksiin ja auditointihavaintojen jatkotoimiin. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Kartoitettu johdon katselmoinnin suunnitteluun, PIMS:n suorituskyvyn katselmointiin, auditointi- ja korjaavien toimenpiteiden trendien katselmointiin, tuotosten hyväksymiseen ja resurssipäätöksiin. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Kartoitettu jatkuvan parantamisen mahdollisuuksien tunnistamiseen, hyväksymiseen, toteuttamiseen ja seurantaan PIMS:n soveltuvuuden, riittävyyden ja vaikuttavuuden osalta. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Kartoitettu poikkeamien kirjaamiseen, juurisyyanalyysiin, korjaavien toimenpiteiden suunnitteluun, korjaavien toimenpiteiden toteutukseen, vaikuttavuuden varmentamiseen, eskalointiin ja soveltamiseen. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Kartoitettu rekisterinpitäjän käsittelytallenteisiin, joita käytetään todentavan aineiston lähteinä seurannassa, auditoinnin otannassa ja käsittelytoimien luettelon ajantasaisuusmittareissa. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Kartoitettu henkilötietojen käsittelijän sopimukseen, asiakkaan auditointiin, varmentamisvastaukseen ja henkilötietojen käsittelijän yhteistyönäyttöön, joita seurataan toimittaja- ja asiakasvarmennusprosessien kautta. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartoitettu osoitusvelvollisuuden todentavaan aineistoon seurannasta, auditoinnista, johdon katselmoinnista, korjaavista toimenpiteistä ja jatkuvasta parantamisesta. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän hallinnointitoimenpiteisiin, vaikuttavuuden katselmointiin, johdon katselmointiin, korjaaviin toimenpiteisiin ja dokumentoituun parantamisnäyttöön. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Kartoitettu henkilötietojen käsittelijää, alikäsittelijää, asiakkaan auditointia, kolmannen osapuolen varmentamista ja toimittajayhteistyötä koskevaan todentavaan aineistoon. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Kartoitettu käsittelytallenteisiin, joita käytetään seurannan, auditoinnin otannan, näyttöobjektien täydellisyyden ja käsittelytoimien luettelon ajantasaisuuden näyttönä. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Kartoitettu henkilötietojen tietoturvakontrollien tilan, teknisten kontrollien näytön ja tietoturvaan liittyvän vaikuttavuusnäytön seurantaan ja arviointiin. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Kartoitettu Data Protection Officer / Privacy Advisor -roolin tietosuojaneuvontaan, seurantahavaintoihin, auditoinnin tukeen ja tietosuojan

vaatimustenmukaisuustrendien katselmointiin soveltuvin osin. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Kartoitettu tietosuojan vaatimustenmukaisuuden todentamiseen, sisäisiin tai riippumattomiin auditointeihin, sisäisiin kontrolleihin, valvontamekanismeihin ja tietosuojariskien arvioinnin todentavaan aineistoon. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Kartoitettu henkilötietoihin liittyvän tietoturvallisuuden riippumattomaan katselmointiin, politiikkojen ja standardien noudattamiseen sekä henkilötietojen suojauksen teknisen vaatimustenmukaisuuden katselmointiin. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Kartoitettu tietoturvallisuuden seuranta- ja arviointilähtötietoihin, jotka tukevat PIMS:n suorituskyvyn mittaamista ja henkilötietojen tietoturvakontrollien tilaa. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Kartoitettu ISMS:n sisäisen auditoinnin tukeen PIMS-auditoinnin suunnittelussa, auditointinäytössä, auditointituloksissa ja auditointiohjelman valmistumisessa. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Kartoitettu johdon katselmoinnin lähtötietoihin ja tuotoksiin PIMS:n ja tietoturvallisuuden suorituskyvyn integroidussa valvonnassa. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Kartoitettu PIMS:n ja sitä tukevan tietoturvakontrolliympäristön jatkuvaan parantamiseen. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Kartoitettu poikkeamien käsittelyyn, korjaavien toimenpiteiden suunnitteluun, korjaavien toimenpiteiden toteutukseen ja vaikuttavuuden varmentamiseen. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Kartoitettu riippumattomaan katselmointiin, auditoijan riippumattomuuden tarkastuksiin, auditointinäytön testaamiseen ja korjaavien toimenpiteiden vaikuttavuuden riippumattomaan varmentamiseen. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Kartoitettu PIMS- ja tietoturvapolitiikkojen vaatimustenmukaisuuden katselmointiin, kontrollien toteutuksen tilaan ja standardien mukaisuuden näyttöön. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Kartoitettu auditoinnin periaatteisiin, auditointiohjelman hallintaan, auditoinnin toteuttamiseen, näyttöön perustuvaan auditointiraportointiin, auditoinnin jatkotoimiin ja PIMS-auditointien auditoijien pätevyysodotuksiin. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].