					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII15					Asiakirjan nimi: **Henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten 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 7.4; Clause 7.5	Both	Supporting	PIMS-viestintä ja dokumentoitu henkilötietojen tietoturvaloukkausta koskeva todentava aineisto
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operatiivinen ohjaus sekä yhteys tietosuojariskien arviointiin ja tietosuojariskien käsittelyyn
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seuranta, arviointi, poikkeama, korjaavat toimenpiteet ja parantaminen
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Poikkeamien hallinnan suunnittelu ja valmistautuminen PII:n käsittelyä varten
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reagointi PII:tä koskeviin tietoturvapoikkeamiin
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Laki-, lakisääteiset, sääntely- ja sopimusvaatimukset sekä tallenteiden suojaaminen
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Henkilötietojen käsittelijän asiakassopimus ja asiakkaan velvoitteiden tukeminen
GDPR	Article 5(2); Article 24	Controller	Supporting	Osoitusvelvollisuus ja rekisterinpitäjän vastuu
GDPR	Article 26	Joint Controller	Supporting	Yhteisrekisterinpitäjien tietoturvaloukkausvastuiden koordinointi
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijän avustaminen ja käsittelijäsopimuksen velvoitteet
GDPR	Article 32	Both	Supporting	Käsittelyn turvallisuus ja tietoturvaloukkausten havaitsemiskyky
GDPR	Article 33	Both	Primary	Henkilötietojen tietoturvaloukkauksesta ilmoittaminen ja loukkauksen dokumentointi

GDPR	Article 34	Controller	Primary	Henkilötietojen tietoturvaloukkausten viestintä asianomaisille rekisteröidyille
GDPR	Article 39	Conditional	Supporting	DPO:n neuvonta, seuranta, yhteistyö ja yhteyspisteen tuki
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Tietoturvan ja tietosuojan vaatimustenmukaisuuden periaatteet
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Henkilötietopoikkeamiin reagoinnin vastuut ja tapahtumien raportointi
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Poikkeamiin varautuminen, arviointi, reagointi, opit ja todistusaineiston kerääminen
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Poikkeamien hallintaprosessin elinkaari
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Poikkeamapolitiikka, suunnitelma, tietoisuus, testaus ja opit
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Havaitseminen, ilmoittaminen, triage, analyysi, reagointi ja raportointitoiminnot
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Pilvipalvelun henkilötietojen käsittelijän ilmoitus- ja loukkaustallennevaatimukset
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Merkittävien poikkeamien raportointi soveltuvin osin
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	ICT-poikkeamien hallinta, luokittelu ja raportointi soveltuvin osin

1. Soveltamisala

1.1 Tässä politiikassa määritetään vaatimukset PIMS:n soveltamisalaan kuuluvien henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten tunnistamiselle, ilmoittamiselle, triage-käsittelylle, arvioinnille, rajaamiselle, ilmoittamiselle viranomaisille ja muille tahoille, dokumentoinnille, sulkemiselle sekä niistä oppimiselle.

1.2 Tätä politiikkaa sovelletaan seuraaviin:

1.2.1 organisaatio toimii PII:n rekisterinpitäjänä;

1.2.2 organisaatio toimii yhteisrekisterinpitäjänä, kun tietoturvaloukkausvastuiden koordinointia edellytetään;

1.2.3 organisaatio toimii PII:n henkilötietojen käsittelijänä;

1.2.4 organisaatio toimii alikäsittelijänä;

1.2.5 järjestelmät, sovellukset, palvelut, prosessit, toimittajat, henkilötietojen käsittelijät, alikäsittelijät ja kolmannet osapuolet, jotka käsittelevät, tallentavat, siirtävät, tukevat, käyttävät tai muutoin vaikuttavat PII:hin PIMS:n soveltamisalassa.

1.3 Tässä politiikassa käytetään REG10 - Henkilötietopoikkeama- ja tietoturvaloukkausrekisteriä ensisijaisena todentavan aineiston kohteena henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallinnassa.

1.4 Tässä politiikassa käytetään tukevia todentavan aineiston kohteita seuraavasti:

1.4.1 REG01 PIMS:n soveltamisalaa sekä sovellettavien sidosryhmien, oikeudellisten, sopimusperusteisten, toimialakohtaisten ja asiakasraportointia koskevien kontekstien kuvaamiseen.

1.4.2 REG02 asianomaisten käsittelytoimien, PII-luokkien, rekisteröityjen luokkien, tarkoitusten ja järjestelmien kuvaamiseen.

1.4.3 REG03 soveltuvuuslausunnon ja kontrollien sovellettavuuden päivityksiin.

1.4.4 REG04 tietosuojariskin, DPIA:n ja jäännösriskin yhteyksiin.

1.4.5 REG08 henkilötietojen käsittelijöiden, alikäsittelijöiden, asiakkaiden, toimittajien ja kolmansien osapuolten poikkeamarajapintaa koskevaan todentavaan aineistoon.

1.4.6 REG09 henkilötietojen kansainvälisten siirtojen yhteyksiin, kun poikkeama vaikuttaa rajat ylittävään käsittelyyn.

1.4.7 REG11 koulutusta, tietoisuutta ja poikkeamiin reagoinnin osaamista koskevaan todentavaan aineistoon.

1.4.8 REG12 auditointia, poikkeamia, korjaavia toimenpiteitä ja parantamista koskevaan todentavaan aineistoon.

1.5 Tämä politiikka tukeutuu liittyviin PIMS-politiikkoihin erityiskontrollien osalta:

1.5.1 PII03 ohjaa käsittelytoimien luetteloa ja oikeusperustetallenteita.

1.5.2 PII04 ohjaa tietosuojaselostetta ja läpinäkyvyyskontrolleja loukkauskohtaisten viestien ulkopuolella.

1.5.3 PII06 ohjaa rekisteröidyn oikeuksia koskevia pyyntöjä, jotka syntyvät ennen poikkeamaa, sen aikana tai sen jälkeen.

1.5.4 PII07 ohjaa tietosuojariskien arvioinnin ja DPIA:n menetelmää.

1.5.5 PII08 ohjaa sisäänrakennetun ja oletusarvoisen tietosuojan kontrolleja.

1.5.6 PII10 ohjaa säilytyksen, poistamisen ja hävittämisen kontrolleja.

1.5.7 PII12 ohjaa henkilötietojen käsittelijöihin, alikäsittelijöihin, toimittajiin ja kolmansien osapuolten tietosuojasuhteisiin liittyviä kontrolleja.

1.5.8 PII13 ohjaa henkilötietojen kansainvälisiä siirtoperusteita ja siirtoriskitallenteita.

1.5.9 PII14 ohjaa ennaltaehkäiseviä ja havaitsevia PII:n tietoturva- ja pääsynhallintakontrolleja.

1.5.10 PII16 ohjaa tietosuojakoulutusta, tietoisuutta ja osaamista.

1.5.11 PII17 ohjaa dokumentoitua tietoa ja todentavan aineiston hallintaa.

1.5.12 PII18 ohjaa seurantaa, sisäistä auditointia, johdon katselmointia, poikkeamia, korjaavia toimenpiteitä ja jatkuvaa parantamista.

1.6 Tässä politiikassa sovelletaan seuraavia määritelmiä:

1.6.1 "Henkilötietopoikkeama" tarkoittaa epäiltyä tai vahvistettua tapahtumaa, joka on vaikuttanut, on voinut vaikuttaa tai voisi kohtuudella vaikuttaa PII:n luottamuksellisuuteen, eheyteen, saatavuuteen, lainmukaiseen käsittelyyn tai luvalliseen käsittelyyn.

1.6.2 "Henkilötietojen tietoturvaloukkaus" tarkoittaa vahvistettua henkilötietopoikkeamaa, johon liittyy PII:n luvaton, lainvastainen, vahingossa tapahtunut tai tahaton tuhoaminen, menettäminen, muuttaminen, luovuttaminen, siihen pääsy, sen saatavuuden estyminen tai sen vaarantuminen.

1.6.3 "Tietoturvaloukkauksen arviointi" tarkoittaa dokumentoitua arviointia siitä, onko henkilötietopoikkeama henkilötietojen tietoturvaloukkaus, mitä PII:tä ja rekisteröityjä se koskee, mitä riskejä voi syntyä, mitä ilmoituksia tai viestintää edellytetään ja mitä korjaavia toimia tarvitaan.

1.6.4 "Tietoisuus tapahtumasta" tarkoittaa ajankohtaa, jolloin organisaatiolla on kohtuullinen varmuus siitä, että tietoturva- tai tietosuojapoikkeama on tapahtunut ja että PII on vaarantunut tai on voinut vaarantua.

1.6.5 "Vaikutuksiltaan merkittävä henkilötietopoikkeama" tarkoittaa henkilötietopoikkeamaa, johon liittyy korkean riskin käsittelyä, erityisiin henkilötietoryhmiin kuuluvaa tai erittäin arkaluonteista PII:tä, laajamittaista PII:tä, haavoittuvassa asemassa olevia henkilöitä, säänneltyjä asiakkaita, useiden lainkäyttöalueiden vaikutuksia, olennaisia asiakasvaikutuksia, etuoikeutetun pääsyn vaarantumista, julkista altistumista, kiristyshaittaohjelmia, palvelun saatavuuden estymistä tai merkittäviä operatiivisia tai mainevaikutuksia.

1.6.6 "Olennainen poikkeamaa koskeva muutos" tarkoittaa uutta tai muuttunutta tietoa, joka vaikuttaa poikkeaman laajuuteen, vakavuuteen, PII-luokkiin, rekisteröityihin kohdistuviin vaikutuksiin, ilmoituspäätökseen, asiakasvaikutukseen, juurisyyhyn, rajaamiseen, palautumiseen, korjaaviin toimenpiteisiin tai ulkoisiin raportointivelvoitteisiin.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että henkilötietopoikkeamat ja henkilötietojen tietoturvaloukkaukset käsitellään yhdenmukaisesti, viipymättä, lainmukaisesti, turvallisesti ja auditointia varten valmiilla todentavalla aineistolla.

2.2 Tämä politiikka tukee osoitusvelvollisuutta edellyttämällä, että henkilötietopoikkeamat ja henkilötietojen tietoturvaloukkaukset kirjataan REG10:een ja yhdistetään tarvittaessa asianomaisiin käsittelytallenteisiin, tietosuojariskeihin, henkilötietojen käsittelijä- ja alikäsittelijäsuhteisiin, siirtotallenteisiin, korjaaviin toimenpiteisiin ja koulutustallenteisiin.

2.3 Tämä politiikka varmistaa, että rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän velvoitteet käsitellään erillisten sovellettavuussääntöjen mukaisesti, mutta yhden integroidun poikkeama- ja tietoturvaloukkausnäyttömallin avulla.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 varmistaa, että epäillyt henkilötietopoikkeamat ilmoitetaan ja kirjataan viipymättä;

3.1.2 varmistaa, että henkilötietopoikkeamat käsitellään triage-menettelyssä ja luokitellaan yhdenmukaisin kriteerein;

3.1.3 varmistaa, että tietoturvaloukkauksen arvioinneissa huomioidaan asianomainen PII, rekisteröidyt, järjestelmät, käsittelytoimet, henkilötietojen käsittelijät, alikäsittelijät, siirrot, riskit ja korjaavat toimet;

3.1.4 varmistaa, että rekisterinpitäjän ilmoituspäätökset ja rekisteröidyille suunnattua viestintää koskevat päätökset dokumentoidaan;

3.1.5 varmistaa, että henkilötietojen käsittelijän ja alikäsittelijän tietoturvaloukkausilmoitukset asiakkaille tai ylemmän tason osapuolille tehdään ilman aiheetonta viivytystä ja sovellettavien sopimusten mukaisesti;

3.1.6 varmistaa, että todentava aineisto säilytetään ja suojataan poikkeaman käsittelyn aikana;

3.1.7 varmistaa, että rajaaminen, poistaminen, palautuminen ja validointi seurataan REG10:n kautta;

3.1.8 varmistaa, että säännellyt, sopimusperusteiset, asiakas- ja toimialakohtaiset raportointikynnykset arvioidaan soveltuvin osin;

3.1.9 varmistaa, että poikkeamista saadut opit johtavat korjaaviin toimenpiteisiin ja jatkuvaan parantamiseen;

3.1.10 varmistaa, että poikkeama- ja tietoturvaloukkaustallenteet ovat saatavilla auditointia, johdon katselmointia, asiakkaiden varmentamista ja viranomaistarkastelua varten soveltuvin osin.

4. Politiikkalausumat

4.1 Valmius poikkeamatilanteisiin ja vastaanotto

4.1.1 [Both] Privacy Lead / PIMS Manager tulee ylläpitää henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten käsittelykriteerejä REG10:ssä vähintään vuosittain ja aina PIMS:n soveltamisalan, oikeudellisen kontekstin, sopimusvelvoitteiden tai korkean riskin käsittelyn olennaisen muutoksen jälkeen.

4.1.2 [All] Incident Response Coordinator tulee kirjata jokainen ilmoitettu tai havaittu epäilty henkilötietopoikkeama REG10:een yhden työpäivän kuluessa vastaanottamisesta tai aiemmin, jos sovellettava ilmoitus- tai asiakasraportoinnin määräaika voi käynnistyä.

4.1.3 [Both] System Owner / Application Owner tulee säilyttää REG10:een linkitetyt asiaankuuluvat järjestelmälokit, hälytykset, käyttöoikeustallenteet, konfiguraationäyttö ja palautumisnäyttö, kun epäilty poikkeama vaikuttaa PII:tä käsittelevään järjestelmään tai sovellukseen.

4.1.4 [Both] Information Security Lead tulee tehdä PII:tä koskevan tietoturvatapahtuman alustava tekninen triage 24 tunnin kuluessa havaitsemisesta ja kirjata alustava vakavuus, asianomaiset omaisuuserät ja rajaamisen tila REG10:een.

4.2 Luokittelu ja tietoturvaloukkauksen arviointi

4.2.1 [Both] Incident Response Coordinator tulee luokitella jokainen REG10-merkintä ei-PII-tapahtumaksi, epäillyksi henkilötietopoikkeamaksi, vahvistetuksi henkilötietopoikkeamaksi tai vahvistetuksi henkilötietojen tietoturvaloukkaukseksi 24 tunnin kuluessa vastaanotosta tai päivittää REG10-tallenteeseen syy, miksi luokittelu on edelleen kesken.

4.2.2 [Both] Privacy Lead / PIMS Manager tulee tunnistaa asianomainen käsittelytoimi, PII-luokat, rekisteröityjen luokat, järjestelmät, henkilötietojen käsittelijät, alikäsittelijät, siirtosijainnit ja tietosuojariskit REG02:ssa, REG04:ssä, REG08:ssa, REG09:ssä ja REG10:ssä ennen kuin tietoturvaloukkausta koskeva ilmoituspäätös viimeistellään.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor tulee arvioida asianomaisiin rekisteröityihin kohdistuva riski jokaisesta vahvistetusta tai perustellusti epäillystä

henkilötietojen tietoturvaloukkauksesta ja kirjata ilmoitussuositus, riskiperuste ja neuvonta REG10:een ennen ulkoista ilmoituspäätöstä.

4.2.4 [Processor] Privacy Lead / PIMS Manager tulee tunnistaa asianomainen rekisterinpitäjä tai asiakas ja sovellettavat sopimusperusteiset ilmoitusvaatimukset heti, kun organisaatio tulee tietoiseksi asiakkaan PII:hin vaikuttavasta henkilötietojen tietoturvaloukkauksesta, ja tulos tulee kirjata REG08:aan ja REG10:een.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager tulee varmistaa sovittu tietoturvaloukkausvastuu, johtava viestintävastuu ja koordinointijärjestely ennen yhteisrekisterinpitäjän tekemää ulkoista ilmoitusta tai viestintää, ja päätös tulee kirjata REG08:aan ja REG10:een.

4.2.6 [Conditional] Privacy Lead / PIMS Manager tulee arvioida sovellettavat oikeudelliset, toimialakohtaiset, finanssisektorin, kyberturvallisuuden, sopimusperusteiset, asiakas- ja palvelunsaajaraportoinnin käynnistävät tekijät jokaisen vaikutuksiltaan merkittävän henkilötietopoikkeaman osalta ja kirjata sovellettavuuden tulos REG01:een, REG08:aan ja REG10:een.

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

9. Poikkeukset

9.1.1 [Both] Privacy Lead / PIMS Manager tulee kirjata kaikki tähän politiikkaan tehtävät poikkeukset REG12:een ennen toteutusta tai 24 tunnin kuluessa hätätoimesta, jos ennakkohyväksyntä ei ollut mahdollinen.

9.1.2 [Both] Top Management tulee hyväksyä ennen poikkeaman sulkemista jokainen poikkeus, joka olennaisesti vaikuttaa tietoturvaloukkauksesta ilmoittamisen ajoitukseen, julkiseen viestintään, asiakassitoumukseen, todentavan aineiston säilyttämiseen tai rekisteröityyn kohdistuvaan riskiin, ja hyväksyntänäyttö tulee säilyttää REG10:ssä ja REG12:ssa.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor tulee dokumentoida neuvonta jokaisesta viivästetystä ilmoituksesta, ilmoittamatta jättämisen päätöksestä tai poikkeuksellisesta viestintätavasta ennen poikkeaman sulkemista, ja neuvonta tulee säilyttää REG10:ssä.

9.1.4 [Both] Vendor / Procurement Owner tulee kirjata toimittajan, henkilötietojen käsittelijän, alikäsittelijän tai asiakkaan aiheuttamat poikkeukset, jotka vaikuttavat poikkeamiin reagointiin, REG08:aan ja REG12:een viiden työpäivän kuluessa poikkeuksen tunnistamisesta.

10. Soveltaminen

10.1.1 [All] Process Owner / Business Owner tulee eskaloida epäillystä henkilötietopoikkeamasta ilmoittamatta jättäminen, todentavan aineiston säilyttämisen laiminlyönti, osoitettujen toimien noudattamatta jättäminen tai tietoturvaloukkauksen arviointiin osallistumatta jättäminen roolille Privacy Lead / PIMS Manager kahden työpäivän kuluessa havaitsemisesta, ja todentava aineisto tulee säilyttää REG12:ssa.

10.1.2 [Both] Privacy Lead / PIMS Manager tulee kirjata REG12-poikkeama, kun tämän politiikan rikkominen vaikuttaa poikkeaman vastaanottoon, triageen, rajaamiseen, ilmoittamiseen, todistusaineiston eheyteen, viestintään tai korjaaviin toimenpiteisiin.

10.1.3 [Both] Vendor / Procurement Owner tulee käynnistää toimittajan tai henkilötietojen käsittelijän korjaavat toimet REG08:n ja REG12:n kautta viiden työpäivän kuluessa, kun henkilötietojen käsittelijä, alikäsittelijä, toimittaja tai muu kolmas osapuoli ei täytä sovittuja poikkeama- tai tietoturvaloukkausvelvoitteita.

10.1.4 [Both] Top Management tulee katselmoida olennaiset tai toistuvat poikkeamien hallinnan poikkeamat seuraavassa suunnitellussa johdon katselmoinnissa, ja päätökset sekä vaaditut toimet tulee säilyttää REG12:ssa.

11. Katselmointi ja ylläpito

11.1.1 [Both] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka vähintään vuosittain ja kirjata katselmoinnin tulos, vaaditut muutokset ja hyväksyntätila REG12:een.

11.1.2 [Both] Incident Response Coordinator tulee käynnistää tämän politiikan poikkeaman jälkeinen katselmointi 30 kalenteripäivän kuluessa vaikutuksiltaan merkittävän henkilötietopoikkeaman tai vahvistetun henkilötietojen tietoturvaloukkauksen sulkemisesta, ja katselmointinäyttö tulee säilyttää REG10:ssä ja REG12:ssa.

11.1.3 [Conditional] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka 30 kalenteripäivän kuluessa siitä, kun se tulee tietoiseksi olennaisesta muutoksesta sovellettaviin oikeudellisiin, toimialakohtaisiin, asiakas-, sopimusperusteisiin, henkilötietojen käsittelijää, alikäsittelijää tai siirtoja koskeviin poikkeamaraportoinnin vaatimuksiin, ja katselmointinäyttö tulee säilyttää REG01:ssä, REG08:ssa, REG09:ssä ja REG12:ssa.

11.1.4 [Both] Internal Audit / Compliance Reviewer tulee tarkastaa tämän politiikan toteutus vähintään vuosittain PIMS:n sisäisen auditointiohjelman kautta, ja auditointihavainnot sekä korjaavat toimenpiteet tulee säilyttää REG12:ssa.

11.1.5 [Both] Top Management tulee katselmoida poikkeamatrendit, merkittävät tietoturvaloukkaukset, ilmoitusten suorituskyky, viivästyneet korjaavat toimenpiteet ja politiikan vaikuttavuus suunnitellussa johdon katselmoinnissa, ja tuotokset tulee säilyttää REG12:ssa.

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 - PII:n käsittelytoimien luettelon ja oikeusperusteen politiikka

12.5 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.6 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.7 PII07 - Tietosuojariskien arvioinnin ja DPIA:n politiikka

12.8 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.9 PII10 - PII:n säilytys-, poistamis- ja hävityspolitiikka

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

12.11 PII13 - Henkilötietojen kansainvälisen siirron politiikka

12.12 PII14 - PII:n tietoturva- ja pääsynhallintapolitiikka

12.13 PII16 - Tietosuojakoulutus-, tietoisuus- ja osaamispolitiikka

12.14 PII17 - PIMS:n dokumentoidun tiedon ja todentavan aineiston hallinnan politiikka

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

13. Viitestandardit ja viitekehykset

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].