					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII14					Asiakirjan nimi: **PII:n tietoturva- ja pääsynhallintapolitiikka**							
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 6.1.3; Clause 8.1	Both	Primary	PII:n tietoturvakontrollien suunnittelu ja käyttö
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Näyttö, seuranta ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identiteetti ja käyttöoikeudet PII:n käsittelyssä
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Päätelaitesuojaus ja turvallinen todennus
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Lokitus ja kryptografinen suojaus
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Sovellusturvallisuus ja turvallinen arkkitehtuuri
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Tallenteiden suojaus ja katselmointi
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Turvallisuus, osoitusvelvollisuus ja henkilötietojen käsittelijää koskevat kontrollit
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	ISMS-kontrollien integrointi
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Tietoturvakontrollien toteutusta koskeva ohjeistus
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Tietoturvan ja tietosuojan vaatimustenmukaisuuden periaatteet
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2;	Both	Supporting	PII:n suojaamisen tietoturvakontrollit

	Clause 18.2.3; Clause 18.2.4			

1. Soveltamisala

1.1 Tämä politiikka määrittää PII-kohtaiset tietoturva- ja pääsynhallintavaatimukset järjestelmille, sovelluksille, palveluille, laitteille, pilviympäristöille ja operatiivisille prosesseille, jotka tallentavat, siirtävät, käsittelevät, käyttävät, ylläpitävät tai suojaavat PII:tä.

1.2 Tätä politiikkaa sovelletaan rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän konteksteissa, joissa organisaatio määrittää, käyttää, tukee tai hyödyntää PII:n käsittelyn tietoturvakontrolleja.

1.3 Tämä politiikka kattaa seuraavat PII:n tietoturvakontrollien osa-alueet:

1.3.1 PII:n tietoturvan perustaso ja integrointi olemassa oleviin tietoturvapolitiikkoihin;

1.3.2 pääsynhallinta;

1.3.3 todennus;

1.3.4 etuoikeutetut käyttöoikeudet;

1.3.5 salaus ja turvallinen säilytys;

1.3.6 lokitus ja seuranta;

1.3.7 turvallinen konfigurointi ja haavoittuvuuksien hallinta;

1.3.8 päätelaitteiden ja pilvipalvelujen pääsynhallintakontrollit;

1.3.9 näytön linkitys REG02-, REG08-, REG10- ja REG12-objektien kautta.

1.4 Tämä politiikka ei korvaa kattavaa tietoturvallisuuden hallintajärjestelmää, verkkoturvallisuuspolitiikkaa, turvallisen kehityksen politiikkaa, varmuuskopiointipolitiikkaa, päätelaitepolitiikkaa, pilviturvallisuuspolitiikkaa, kryptografista standardia, haavoittuvuuksien hallinnan menettelyä tai tietoturvapoikkeamiin reagoinnin menettelyä. Kun tällaiset politiikat ovat jo olemassa, tämä politiikka määrittää PIMS-varmennukseen tarvittavat PII-kohtaiset yhteydet ja näyttövaatimukset.

1.5 Tämä politiikka ei monista seuraavia:

1.5.1 PII:n käsittelytoimien luettelo ja oikeusperusteen omistajuus PII03:ssa;

1.5.2 tietosuojariskien ja DPIA:n menetelmä PII07:ssä;

1.5.3 sisäänrakennetun tietosuojan portit PII08:ssa;

1.5.4 keräämistä, käyttöä, luovutusta ja jakamista koskevat säännöt PII09:ssä;

1.5.5 säilytyksen, poistamisen ja hävittämisen toteutus PII10:ssä;

1.5.6 henkilötietojen käsittelijän elinkaaren hallinnointi PII12:ssa;

1.5.7 henkilötietojen kansainvälisen siirron siirtoperustetta koskevat kontrollit PII13:ssa;

1.5.8 poikkeama- ja tietoturvaloukkaustyönkulku PII15:ssä;

1.5.9 dokumentoidun tiedon hallinnointi PII17:ssä;

1.5.10 PIMS:n seurannan, auditoinnin ja parantamisen hallinnointi PII18:ssa.

1.6 Tässä politiikassa operatiiviset lokit, tietoturvatyökalujen tulosteet, käyttöoikeuskatselmointien viennit, haavoittuvuusraportit ja konfiguraationäyttö ovat näyttölähteitä, jotka liitetään kanonisiin näyttöobjekteihin, tiivistetään niihin tai joihin niissä viitataan. Ne eivät ole erillisiä PIMS-rekistereitä.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että PII suojataan asianmukaisilla, riskiperusteisilla ja auditoitavissa olevilla tietoturva- ja pääsynhallintakontrolleilla koko käsittelyn ajan.

2.2 Tämä politiikka mahdollistaa sen, että organisaatio voi osoittaa PII:n tietoturvakontrollien olevan suunniteltuja, toteutettuja, katselmoituja, seurattuja ja parannettuja REG02-, REG08-, REG10- ja REG12-objektien kautta ilman päällekkäisten tietoturvarekisterien luomista tai olemassa olevien tietoturvapolitiikkojen korvaamista.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää PII:n pääsynhallinnan perustaso järjestelmille ja käsittelytoimille;

3.1.2 varmistaa, että todennuskontrollit ovat asianmukaisia PII:n arkaluonteisuuden ja pääsykontekstin kannalta;

3.1.3 määrittää etuoikeutettujen ja tavanomaisten PII-käyttöoikeuksien katselmointivaatimukset;

3.1.4 määrittää salauksen ja turvallisen säilytyksen odotukset lepotilassa olevalle ja siirrettävälle PII:lle sekä asiaankuuluvissa pilvi- tai päätelaitekonteksteissa;

3.1.5 määrittää odotukset PII:hin pääsyn, PII:tä koskevien muutosten ja PII:n ylläpidon lokitukselle ja seurannalle;

3.1.6 määrittää turvallisen konfiguroinnin ja haavoittuvuusnäytön vaatimukset PII:tä käsitteleville järjestelmille;

3.1.7 määrittää päätelaite- ja pilvipääsyn odotukset ilman kattavan päätelaite- tai pilviturvallisuuspolitiikan luomista;

3.1.8 linkittää epäillyt PII:tä koskevat tietoturvapoikkeamat REG10:een ilman poikkeamatyönkulun monistamista;

3.1.9 integroitua olemassa oleviin tietoturvapolitiikkoihin, kun niitä on saatavilla;

3.1.10 ylläpitää valmiutta auditointia varten käyttämällä vain REG02-, REG08-, REG10- ja REG12-objekteja.

4. Politiikkalausumat

4.1 PII:n tietoturvan perustaso ja ISMS-integraatio

4.1.1 [Both] Information Security Lead MUST määrittää PII:n tietoturvan perustaso jokaiselle PII:tä käsittelevälle järjestelmälle tai palvelulle REG12:ssa ennen kuin järjestelmä tai palvelu siirtyy tuotantoon tai muuttuu olennaisesti.

4.1.2 [Both] System Owner / Application Owner MUST kirjata toteutetun PII:n tietoturvakontrollinäytön sijainti REG12:ssa ennen kuin olemassa olevaan tietoturvakontrolliin tukeudutaan PIMS-varmennuksessa.

4.1.3 [Controller] Process Owner / Business Owner MUST tunnistaa PII:n arkaluonteisuus, käsittelykonteksti ja pääsytarve REG02:ssa ennen uuden tai olennaisesti muuttuneen PII-käyttöoikeuden pyytämistä.

4.1.4 [Processor] Vendor / Procurement Owner MUST kirjata asiakkaan tietoturvaohjeet, asiakkaan vastuun rajat ja henkilötietojen käsittelijän tietoturvasitoumukset REG08:ssa ennen kuin henkilötietojen käsittelijän pääsy asiakkaan PII:hin alkaa tai muuttuu olennaisesti.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST varmistaa, että PII:n tietoturvanäyttö on linkitetty REG02-, REG08-, REG10- tai REG12-objektiin ennen käsittelytoimen hyväksymistä PIMS-auditoitavaksi.

4.2 Pääsynhallinnan perustaso

4.2.1 [Both] System Owner / Application Owner MUST rajoittaa pääsyn PII:hin hyväksyttyihin rooleihin ja valtuutettuihin käyttäjiin, jotka on kirjattu REG02:ssa tai REG12:ssa tai ovat jäljitettävissä niihin, ennen käyttöoikeuden käyttöönottoa.

4.2.2 [Both] Process Owner / Business Owner MUST hyväksyä PII-käyttöoikeuden liiketoimintatarkoitus REG02:ssa tai REG12:ssa ennen kuin System Owner / Application Owner myöntää käyttöoikeuden.

4.2.3 [Both] System Owner / Application Owner MUST katselmoida käyttäjien pääsyä järjestelmiin, jotka käsittelevät suuren vaikutuksen tai arkaluonteista PII:tä, vähintään neljännesvuosittain ja kirjata katselmoinnin tulos REG12:ssa.

4.2.4 [Both] System Owner / Application Owner MUST katselmoida käyttäjien pääsyä muihin PII:tä käsitteleviin järjestelmiin vähintään vuosittain ja kirjata katselmoinnin tulos REG12:ssa.

4.2.5 [Both] System Owner / Application Owner MUST poistaa tai muuttaa PII-käyttöoikeus REG12:ssa yhden työpäivän kuluessa roolimuutoksesta, työsuhteen päättymisestä, sopimuksen päättymisestä tai siitä, kun käyttöoikeutta ei enää tarvita.

4.2.6 [Processor] Vendor / Procurement Owner MUST vahvistaa REG08:ssa, että henkilötietojen käsittelijän pääsy asiakkaan PII:hin rajoittuu dokumentoituihin asiakkaan ohjeisiin, ennen käyttöoikeuden käyttöönottoa tai muuttamista.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST vahvistaa REG08:ssa, että alikäsittelijän pääsy PII:hin rajoittuu valtuutettuihin alikäsittelytoimiin, ennen alikäsittelijän käyttöoikeuden käyttöönottoa tai muuttamista.

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

9. Poikkeukset

9.1.1 [Both] Information Security Lead MUST kirjata jokainen PII:n tietoturva- tai pääsynhallintavaatimusta koskeva poikkeus REG12:ssa ennen poikkeuksen aktivointia.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST neuvoa korkeamman riskin PII:n tietoturvapoikkeuksissa REG12:ssa ennen hyväksyntää.

9.1.3 [Both] Top Management MUST hyväksyä PII:n tietoturvapoikkeukset REG12:ssa ennen aktivointia, kun poikkeus vaikuttaa suuren vaikutuksen PII:hin, arkaluonteiseen PII:hin, etuoikeutettuihin käyttöoikeuksiin, salaukseen, lokitukseen tai ratkaisemattomiin korkean riskin haavoittuvuuksiin.

9.1.4 [Both] Information Security Lead MUST määrittää poikkeuksen päättymispäivä, korvaava kontrolli ja katselmointipäivä REG12:ssa ennen poikkeuksen hyväksyntää.

9.1.5 [Both] System Owner / Application Owner MUST korjata, uusia tai sulkea vanhentuneet PII:n tietoturvapoikkeukset REG12:ssa viiden työpäivän kuluessa päättymisestä.

9.1.6 [Processor] Vendor / Procurement Owner MUST kirjata asiakkaan PII:hin vaikuttavat henkilötietojen käsittelijän tai alikäsittelijän tietoturvapoikkeukset REG08:ssa ja REG12:ssa ennen hyväksymistä.

10. Soveltaminen

10.1.1 [Both] Privacy Lead / PIMS Manager MUST kirjata poikkeamat puuttuvasta tai puutteellisesta PII:n tietoturvanäytöstä REG12:ssa viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [Both] Information Security Lead MUST osoittaa korjaamisen omistajuus PII:n tietoturvakontrollien epäonnistumisille REG12:ssa viiden työpäivän kuluessa validoinnista.

10.1.3 [Both] System Owner / Application Owner MUST poistaa käytöstä tai rajoittaa luvaton, liiallinen tai ilman näyttöä oleva PII-käyttöoikeus yhden työpäivän kuluessa validoinnista ja kirjata toimenpide REG12:ssa.

10.1.4 [Conditional] Incident Response Coordinator MUST linkittää soveltamistoimet REG10:een yhden työpäivän kuluessa, kun asia koskee epäiltyä tai vahvistettua PII-poikkeamaa.

10.1.5 [Both] Top Management MUST katselmoida toistuvat tai korkean riskin PII:n tietoturvapoikkeamat REG12:ssa ennen johdon katselmointia.

11. Katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager MUST katselmoida tämä politiikka yhdessä Information Security Lead -roolin kanssa vähintään vuosittain ja kirjata katselmoinnin tulos REG12:ssa.

11.1.2 [Both] Information Security Lead MUST katselmoida PII:n tietoturvan perustaso REG12:ssa 30 päivän kuluessa olennaisesta teknologia-, uhka-, auditointi-, poikkeama- tai sääntelymuutoksesta, joka vaikuttaa PII:n tietoturvaan.

11.1.3 [Both] System Owner / Application Owner MUST päivittää järjestelmätason PII:n tietoturvanäyttö REG12:ssa 30 päivän kuluessa olennaisesta arkkitehtuuri-, käyttöoikeus-, konfiguraatio-, haavoittuvuus- tai lokitusmuutoksesta.

11.1.4 [Processor] Vendor / Procurement Owner MUST katselmoida henkilötietojen käsittelijöiden ja alikäsittelijöiden PII:n tietoturvavastuiden näyttö REG08:ssa 30 päivän kuluessa olennaisesta palvelu-, asiakkaan ohjeen tai alikäsittelijän muutoksesta.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST varmistaa politiikan katselmointinäyttö ja valittu PII:n tietoturvakontrollien näyttö REG12:ssa hyväksytyn auditointisuunnitelman mukaisesti.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tulee lukea yhdessä seuraavien kanssa:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka;

12.3 PII02 - Tietosuojaroolien, vastuiden ja vastuuvelvollisuuden politiikka;

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

12.5 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka;

12.6 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka;

12.7 PII09 - PII:n keräämistä, käyttöä, luovutusta ja jakamista koskeva politiikka;

12.8 PII10 - PII:n säilytys-, poistamis- ja hävittämispolitiikka;

12.9 PII12 - Henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojahallinnan politiikka;

12.10 PII13 - PII:n kansainvälisen siirron politiikka;

12.11 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka;

12.12 PII16 - Tietosuojakoulutus-, tietoisuus- ja pätevyyspolitiikka;

12.13 PII17 - PIMS:n dokumentoidun tiedon ja näytön hallintapolitiikka;

12.14 PII18 - PIMS:n seuranta-, auditointi- ja parantamispolitiikka.

13. Viitestandardit ja viitekehykset

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].