| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>PII15-FS | | | | | Asiakirjan nimi:<br>**Finanssialan henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallintapolitiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>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 poikkeamanäyttö |
| ISO/IEC 27701:2025 | Clause 8.1; Clause 8.2; Clause 8.3 | Both | Supporting | Operatiivinen ohjaus sekä yhteys tietosuojariskien arviointiin ja 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 valmistelu henkilötietojen käsittelyä varten |
| ISO/IEC 27701:2025 | Annex A.3.12 | Both | Primary | Reagointi henkilötietoja koskeviin tietoturvapoikkeamiin |
| ISO/IEC 27701:2025 | Annex A.3.13; Annex A.3.14 | Both | Supporting | Oikeudelliset, lakisääteiset, sääntelyyn perustuvat ja sopimusperusteiset vaatimukset 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 tuki |
| GDPR | Article 5(2); Article 24 | Controller | Supporting | Osoitusvelvollisuus ja rekisterinpitäjän vastuu |
| GDPR | Article 26 | Joint Controller | Supporting | Yhteisrekisterinpitäjien poikkeamavastuiden koordinointi |
| GDPR | Article 28 | Both | Supporting | Henkilötietojen käsittelijän avustamis- ja sopimusvelvoitteet |
| GDPR | Article 32 | Both | Supporting | Käsittelyn turvallisuus ja valmius havaita tietoturvaloukkaukset |
| GDPR | Article 33 | Both | Primary | Henkilötietojen tietoturvaloukkauksesta |

| | | | | |
|---|---|---|---|---|
| | | | | ilmoittaminen ja loukkausten dokumentointi |
| GDPR | Article 34 | Controller | Primary | Henkilötietojen tietoturvaloukkauksista ilmoittaminen vaikutuksen kohteena oleville rekisteröidyille |
| GDPR | Article 39 | Conditional | Supporting | DPO:n neuvonta, seuranta, yhteistyö ja yhteyspistetuki |
| DORA Regulation (EU) 2022/2554 | Article 17 | Conditional | Primary | ICT-poikkeamien hallintaprosessi soveltamisalaan kuuluville finanssialan toimijoille |
| DORA Regulation (EU) 2022/2554 | Article 18 | Conditional | Primary | ICT-poikkeamien ja merkittävien kyberuhkien luokittelukriteerit |
| DORA Regulation (EU) 2022/2554 | Article 19 | Conditional | Primary | Vakavista ICT-poikkeamista raportointi ja merkittävistä kyberuhkista ilmoittaminen |
| DORA Regulation (EU) 2022/2554 | Article 20 | Conditional | Supporting | Raportoinnin sisältö, määräajat, mallit ja menettelyt |
| NIS2 Directive (EU) 2022/2555 | Article 23 | Conditional | Supporting | Merkittävistä poikkeamista raportointi soveltuvin osin |
| ISO/IEC 29100:2020 | Clause 5.11; Clause 5.12 | Both | Supporting | Tietoturvan ja tietosuojan noudattamisen periaatteet |
| ISO/IEC 29151:2022 | Clause 16.1.2; Clause 16.1.3 | Both | Supporting | Vastuut henkilötietopoikkeamiin reagoinnissa ja tapahtumista ilmoittamisessa |
| ISO/IEC 27002:2022 | Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28 | Both | Supporting | Poikkeamien suunnittelu, arviointi, reagointi, opit ja todistusaineiston kerääminen |
| ISO/IEC 27035-1:2023 | Clause 5.2; Clause 5.3; Clause 5.4; | Both | Supporting | Poikkeamien hallintaprosessin elinkaari |

| | | | | |
|---|---|---|---|---|
| | Clause 5.5; Clause 5.6 | | | |
| 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 | Havaitsemisen, ilmoittamisen, luokittelun, analyysin, reagoinnin ja raportoinnin toiminnot |
| ISO/IEC 27018:2020 | Annex A.10.1 | Conditional | Supporting | Julkisen pilven henkilötietojen käsittelijän ilmoitus- ja loukkauskirjausodotukset |

## 1. Soveltamisala

1.1 Tämä politiikka määrittää vaatimukset henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten tunnistamiselle, raportoinnille, luokittelulle ja priorisoinnille, luokittelulle, arvioinnille, rajaamiselle, ilmoittamiselle, dokumentoinnille, sulkemiselle ja niistä oppimiselle finanssialan PIMS-soveltamisaloissa.

1.2 **Toteutushuomautus:** Tämä politiikka on PII15:n korvaava finanssialakohtainen variantti. Sitä ei saa toteuttaa samanaikaisesti PII15:n kanssa samalle PIMS-soveltamisalalle, liiketoimintayksikölle, tuotteelle, asiakasympäristölle, säännellylle palvelulle tai näyttörajoille. Organisaatioiden tulee valita samaan soveltamisalaan joko PII15 tai PII15-FS, jotta vältetään päällekkäiset poikkeamienhallintavelvoitteet, päällekkäiset rekisterit ja päällekkäinen auditointinäyttötyö.

**1.3 Tätä politiikkaa sovelletaan:**

1.3.1 organisaatioon, joka toimii rekisterinpitäjänä finanssialan kontekstissa;

1.3.2 organisaatioon, joka toimii yhteisrekisterinpitäjänä, kun poikkeama- tai loukkausvastuiden koordinointi on tarpeen;

1.3.3 organisaatioon, joka toimii henkilötietojen käsittelijänä finanssialan asiakkaille;

1.3.4 organisaatioon, joka toimii alikäsittelijänä finanssialan asiakkaille tai ylemmän tason henkilötietojen käsittelijöille;

1.3.5 järjestelmiin, sovelluksiin, palveluihin, prosesseihin, toimittajiin, henkilötietojen käsittelijöihin, alikäsittelijöihin ja kolmansiin osapuoliin, jotka käsittelevät, säilyttävät, siirtävät, tukevat, käyttävät tai muutoin vaikuttavat henkilötietoihin finanssialan PIMS-soveltamisalassa.

1.4 Tässä politiikassa käytetään REG10 - henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten rekisteriä ensisijaisena näyttöobjektina finanssialan henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallinnassa.

**1.5 Tässä politiikassa käytetään tukevia näyttöobjekteja seuraavasti:**

1.5.1 REG01 PIMS-soveltamisalaa sekä sovellettavaa sidosryhmä-, toimiala-, asiakas-, sopimus- ja raportointikontekstia varten.

1.5.2 REG02 vaikutuksen kohteena olevia käsittelytoimia, henkilötietoryhmiä, rekisteröityjen ryhmiä, käyttötarkoituksia, järjestelmiä ja palveluja varten.

1.5.3 REG03 soveltuvuuslausuntoa ja kontrollien sovellettavuuden päivityksiä varten, mukaan lukien PII15:n korvaaminen PII15-FS:llä samassa soveltamisalassa.

1.5.4 REG04 tietosuojariskin, DPIA:n, jäännösriskin ja riskien käsittelyn yhteyttä varten.

1.5.5 REG08 henkilötietojen käsittelijöiden, alikäsittelijöiden, asiakkaiden, toimittajien ja kolmansien osapuolten poikkeamarajapinnan näyttöä varten.

1.5.6 REG09 kansainvälisen siirron yhteyttä varten, kun poikkeama vaikuttaa rajat ylittävään käsittelyyn.

1.5.7 REG11 koulutusta, tietoisuutta ja poikkeamiin reagoinnin pätevyyttä koskevaa näyttöä varten.

1.5.8 REG12 auditointia, poikkeamia, korjaavia toimenpiteitä, johdon katselmointia ja parantamista koskevaa näyttöä varten.

**1.6 Tämä politiikka tukeutuu asiaan liittyviin PIMS-politiikkoihin erityiskontrollien osalta:**

1.6.1 PII03 ohjaa käsittelytoimien luetteloa ja oikeusperustetallenteita.

1.6.2 PII04 ohjaa tietosuojaselostetta ja läpinäkyvyyskontrolleja loukkauskohtaisen viestinnän ulkopuolella.

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

1.6.4 PII07 ohjaa tietosuojariskien arviointia ja DPIA-menetelmää.

1.6.5 PII08 ohjaa sisäänrakennettua ja oletusarvoista tietosuojaa koskevia kontrolleja.

1.6.6 PII10 ohjaa säilytys-, poisto- ja hävityskontrolleja.

1.6.7 PII12 ohjaa henkilötietojen käsittelijöiden, alikäsittelijöiden, toimittajien ja kolmansien osapuolten tietosuojasuhteiden kontrolleja.

1.6.8 PII13 ohjaa henkilötietojen kansainvälisiä siirtoperusteita ja siirtoriskitallenteita.

1.6.9 PII14 ohjaa ennaltaehkäiseviä ja havaitsevia henkilötietojen tietoturva- ja pääsynhallintakontrolleja.

1.6.10 PII16 ohjaa tietosuojakoulutusta, tietoisuutta ja pätevyyttä.

1.6.11 PII17 ohjaa dokumentoitua tietoa ja näytönhallintaa.

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

1.6.13 PII23 ohjaa pilvipalvelujen henkilötietojen käsittelijäkontrolleja, kun pilvipalvelujen käsittelijävelvoitteet kuuluvat soveltamisalaan.

**1.7 Tässä politiikassa:**

1.7.1 "PII incident" tarkoittaa epäiltyä tai vahvistettua tapahtumaa, joka on vaikuttanut, on voinut vaikuttaa tai voisi kohtuudella vaikuttaa henkilötietojen luottamuksellisuuteen, eheyteen, saatavuuteen, lainmukaiseen käsittelyyn tai valtuutettuun käsittelyyn.

1.7.2 "PII breach" tarkoittaa vahvistettua henkilötietopoikkeamaa, johon liittyy henkilötietojen luvaton, lainvastainen, vahingossa tapahtunut tai tahaton tuhoutuminen, häviäminen, muuttuminen, luovuttaminen, käyttö, saatavuuden menetys tai vaarantuminen.

1.7.3 "Financial-sector PII incident" tarkoittaa henkilötietopoikkeamaa, joka vaikuttaa, voi vaikuttaa tai liittyy kohtuudella säänneltyihin finanssipalveluihin, finanssialan asiakkaisiin, finanssialan vastapuoliin, finanssitapahtumiin, finanssitoimintoihin tai finanssialan henkilötietojen käsittelyyn.

1.7.4 "Major financial-sector incident" tarkoittaa finanssialan henkilötietopoikkeamaa tai siihen liittyvää ICT-poikkeamaa, joka täyttää REG10:ssä dokumentoidut olennaisuus- tai raportointikriteerit.

1.7.5 "Significant cyber threat" tarkoittaa REG10:een kirjattua kyberuhkaa, joka voisi olennaisesti vaikuttaa soveltamisalaan kuuluviin finanssialan palveluihin, henkilötietojen käsittelyyn, asiakkaisiin, vastapuoliin tai toimintoihin.

1.7.6 "Breach assessment" tarkoittaa dokumentoitua arviointia siitä, onko henkilötietopoikkeama henkilötietojen tietoturvaloukkaus, mihin henkilötietoihin ja rekisteröityihin se vaikuttaa, mitä riskejä voi syntyä, mitä ilmoituksia tai viestintää vaaditaan ja mitä korjaavia toimia tarvitaan.

1.7.7 "Awareness" tarkoittaa hetkeä, jolloin organisaatiolla on kohtuullinen varmuus siitä, että tietoturva- tai tietosuojapoikkeama on tapahtunut ja henkilötiedot ovat vaarantuneet tai ovat voineet vaarantua.

1.7.8 "High-impact financial-sector PII incident" tarkoittaa henkilötietopoikkeamaa, johon liittyy korkean riskin käsittelyä, erityisiä henkilötietoryhmiä tai erittäin arkaluonteisia henkilötietoja, laajamittaista henkilötietojen käsittelyä, haavoittuvassa asemassa olevia henkilöitä, säänneltyjä asiakkaita, olennainen palveluhäiriö, finanssialan vastapuolia, finanssitapahtumia, usean lainkäyttöalueen vaikutus, etuoikeutetun pääsyn vaarantuminen, julkinen altistuminen, kiristyshaittaohjelmat, palvelun saatavuuden menetys tai merkittävä operatiivinen, asiakas-, taloudellinen tai mainevaikutus.

1.7.9 "Material incident change" tarkoittaa uutta tai muuttunutta tietoa, joka vaikuttaa poikkeaman soveltamisalaan, vakavuuteen, henkilötietoryhmiin, rekisteröityihin kohdistuvaan vaikutukseen, palveluvaikutukseen, finanssialan luokitteluun, ilmoituspäätökseen, asiakasvaikutukseen, juurisyyhyn, rajaamiseen, palautumiseen, korjaavaan toimenpiteeseen tai ulkoisiin raportointivelvoitteisiin.

## 2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että finanssialan konteksteissa ilmenevät henkilötietopoikkeamat ja henkilötietojen tietoturvaloukkaukset käsitellään johdonmukaisesti, viipymättä, lainmukaisesti, turvallisesti ja auditointia varten valmiilla näytöllä.

2.2 Tämä politiikka tukee osoitusvelvollisuutta edellyttämällä, että finanssialan henkilötietopoikkeamat ja henkilötietojen tietoturvaloukkaukset kirjataan REG10:een ja linkitetään vaikutuksen kohteena oleviin käsittelytallenteisiin, tietosuojariskeihin, henkilötietojen käsittelijä- ja alikäsittelijäsuhteisiin, siirtotallenteisiin, korjaaviin toimenpiteisiin, koulutustallenteisiin, finanssialan raportointipäätöksiin ja johdon katselmointinäyttöön, kun ne laukeavat.

2.3 Tämä politiikka varmistaa, että rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän velvoitteet käsitellään erillisten sovellettavuussääntöjen mukaisesti säilyttäen samalla yksi integroitu finanssialan poikkeama- ja loukkausnäyttömalli.

## 3. Tavoitteet

### 3.1 Tämän politiikan tavoitteena on:

3.1.1 varmistaa, että epäillyistä finanssialan henkilötietopoikkeamista ilmoitetaan ja ne kirjataan viipymättä;

3.1.2 varmistaa, että finanssialan henkilötietopoikkeamat luokitellaan ja priorisoidaan sekä luokitellaan johdonmukaisin tietosuoja-, tietoturva-, operatiivisin ja toimialakohtaisin kriteerein;

3.1.3 varmistaa, että tietoturvaloukkauksen arvioinneissa otetaan huomioon vaikutuksen kohteena olevat henkilötiedot, rekisteröidyt, järjestelmät, palvelut, käsittelytoimet, henkilötietojen käsittelijät, alikäsittelijät, siirrot, riskit, asiakkaat, vastapuolet ja korjaavat toimet;

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

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

3.1.6 varmistaa, että finanssialan raportoinnin laukaisevat tekijät arvioidaan, dokumentoidaan ja niitä seurataan soveltuvin osin;

3.1.7 varmistaa, että näyttö säilytetään ja suojataan poikkeaman käsittelyn aikana;

3.1.8 varmistaa, että rajaamista, hävittämistä, palautumista ja validointia seurataan REG10:n kautta;

3.1.9 varmistaa, että merkittävät kyberuhkat ja merkittävät finanssialan poikkeamat ohjataan asianmukaisiin päätös- ja raportointityönkulkuihin;

3.1.10 varmistaa, että poikkeamista saadut opit johtavat korjaaviin toimenpiteisiin, koulutukseen, kontrollien parantamiseen ja johdon katselmointiin;

3.1.11 varmistaa, että poikkeama- ja loukkaustallenteet ovat käytettävissä auditointia, johdon katselmointia, asiakkaiden varmentamista ja viranomaisarviointia varten soveltuvin osin;

3.1.12 varmistaa, että PII15-FS korvaa PII15:n samassa finanssialan soveltamisalassa eikä aiheuta päällekkäistä PII15-näyttötyötä.

## 4. Politiikkalausumat

### 4.1 Variantin käyttöönotto, valmius ja vastaanotto

4.1.1 [Conditional] Privacy Lead / PIMS Manager tulee dokumentoida PII15-FS:n käyttöönotto REG01:een ja REG03:een ennen tämän politiikan käyttöä finanssialan PIMS-soveltamisalassa.

4.1.2 [Conditional] Privacy Lead / PIMS Manager tulee dokumentoida REG03:een ja REG12:een, ettei PII15:tä toteuteta samanaikaisesti samassa finanssialan PIMS-soveltamisalassa ennen PII15-FS:n hyväksymistä.

4.1.3 [All] Incident Response Coordinator tulee kirjata jokainen ilmoitettu tai havaittu epäilty finanssialan henkilötietopoikkeama REG10:een yhden työpäivän kuluessa vastaanottamisesta tai aiemmin, jos sovellettava ilmoitus-, asiakas- tai raportointiaikataulu voi laueta.

4.1.4 [Conditional] Privacy Lead / PIMS Manager tulee ylläpitää finanssialan henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten käsittelykriteerejä REG10:ssä vähintään vuosittain ja aina PIMS-soveltamisalan, oikeudellisen kontekstin, asiakasvelvoitteiden, sopimusvelvoitteiden, toimialakohtaisen raportointikontekstin tai korkean riskin käsittelyn olennaisen muutoksen jälkeen.

4.1.5 [Both] Information Security Lead tulee vahvistaa poikkeamanäytön säilyttämisvaatimukset REG10:ssä 24 tunnin kuluessa siitä, kun epäilty poikkeama vaikuttaa henkilötietoja käsittelevään järjestelmään, palveluun tai sovellukseen.

4.1.6 [Conditional] Vendor / Procurement Owner tulee ylläpitää finanssialan kolmansien osapuolten poikkeamayhteystietoja ja näytön reititysvaatimuksia REG08:ssa ennen käyttöönottoa ja vähintään vuosittain soveltamisalaan kuuluville henkilötietojen käsittelijöille, alikäsittelijöille, toimittajille ja ulkoistetuille raportointipalveluntarjoajille.

**4.2 Luokittelu ja tietoturvaloukkauksen arviointi**

4.2.1 [All] Incident Response Coordinator tulee luokitella jokainen REG10-kirjaus 24 tunnin kuluessa vastaanotosta seuraavasti: muu kuin henkilötietotapahtuma, epäilty henkilötietopoikkeama, vahvistettu henkilötietopoikkeama, vahvistettu henkilötietojen tietoturvaloukkaus, finanssialan henkilötietopoikkeama, merkittävä finanssialan poikkeama, merkittävä kyberuhka tai luokittelua odottava kirjaus.

4.2.2 [Conditional] Information Security Lead tulee arvioida vaikutuksen kohteena olevat palvelut, asiakkaat, vastapuolet, tapahtumat, palvelun käyttökatko, maantieteellinen levinneisyys, tietojen menetys, palvelun kriittisyys ja taloudellinen vaikutus REG10:ssä, kun henkilötietopoikkeama voi vaikuttaa finanssialan palveluihin tai toimintoihin.

4.2.3 [Both] Privacy Lead / PIMS Manager tulee tunnistaa vaikutuksen kohteena oleva käsittelytoimi, henkilötietoryhmät, rekisteröityjen ryhmät, järjestelmät, henkilötietojen käsittelijät, alikäsittelijät, siirtosijainnit ja tietosuojariskit REG02:ssa, REG04:ssä, REG08:ssa, REG09:ssä ja REG10:ssä ennen kuin loukkausilmoituspäätös viimeistellään.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor tulee arvioida vaikutuksen kohteena oleviin rekisteröityihin kohdistuva riski jokaisessa vahvistetussa tai perustellusti epäillyssä henkilötietojen tietoturvaloukkauksessa sekä kirjata ilmoitussuositus, riskiperuste ja neuvonta REG10:een ennen ulkoisen ilmoituspäätöksen tekemistä.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager tulee kirjata yhteisrekisterinpitäjien poikkeamavastuiden jako REG08:aan ja REG10:een 24 tunnin kuluessa siitä, kun jaettu vastuu epäillystä tai vahvistetusta henkilötietojen tietoturvaloukkauksesta on tunnistettu.

4.2.6 [Processor] Privacy Lead / PIMS Manager tulee arvioida asiakkaan ohjeet, sopimusperusteiset ilmoitusvelvoitteet ja yhteistyövelvoitteet REG08:ssa ja REG10:ssä 24 tunnin kuluessa siitä, kun epäilty tai vahvistettu henkilötietojen tietoturvaloukkaus vaikuttaa henkilötietojen käsittelijänä suoritettavaan käsittelyyn.

4.2.7 [Subprocessor] Vendor / Procurement Owner tulee tunnistaa ylemmän tason ilmoitusketju ja vaadittu näytön reititys REG08:ssa ja REG10:ssä 24 tunnin kuluessa siitä, kun epäilty tai vahvistettu henkilötietopoikkeama vaikuttaa alikäsittelijänä suoritettavaan käsittelyyn.

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

## 9. Poikkeukset

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

9.1.2 [Conditional] Top Management tulee hyväksyä kaikki poikkeukset, jotka olennaisesti vaikuttavat loukkausilmoituksen ajoitukseen, finanssialan raportoinnin ajoitukseen, julkiseen viestintään, asiakassitoumukseen, näytön säilyttämiseen tai rekisteröityyn kohdistuvaan riskiin ennen poikkeaman sulkemista, ja hyväksyntänäyttö säilytetään REG10:ssä ja REG12:ssa.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor tulee dokumentoida neuvonta jokaiselle viivästyneelle ilmoitukselle, ilmoittamatta jättämisen päätökselle, raportointipoikkeukselle tai poikkeukselliselle viestintätavalle ennen poikkeaman sulkemista, ja neuvonta säilytetään REG10:ssä.

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

9.1.5 [All] Privacy Lead / PIMS Manager tulee katselmoida tämän politiikan avoimet poikkeukset vähintään kuukausittain sulkemiseen asti, ja katselmoinnin tila säilytetään REG12:ssa.

## 10. Soveltaminen

10.1.1 [All] Process Owner / Business Owner tulee eskaloida epäillyn finanssialan henkilötietopoikkeaman ilmoittamatta jättäminen, näytön säilyttämättä jättäminen, osoitettujen toimien noudattamatta jättäminen tai tietoturvaloukkauksen arvioinnissa yhteistyöstä kieltäytyminen roolille Privacy Lead / PIMS Manager kahden työpäivän kuluessa havaitsemisesta, ja näyttö säilytetään REG12:ssa.

10.1.2 [Both] Incident Response Coordinator tulee eskaloida myöhäinen ilmoittaminen, puuttuva luokittelu, puuttuva näyttö, puuttuva eskalointi tai erääntynyt rajaamistoimi roolille Privacy Lead / PIMS Manager yhden työpäivän kuluessa ongelman tunnistamisesta, ja näyttö säilytetään REG10:ssä ja REG12:ssa.

10.1.3 [Both] Privacy Lead / PIMS Manager tulee kirjata REG12-poikkeama, kun tämän politiikan rikkominen vaikuttaa poikkeaman vastaanottoon, luokitteluun ja priorisointiin, rajaamiseen, ilmoittamiseen, raportointiin, näytön eheyteen, viestintään tai korjaavaan toimenpiteeseen.

10.1.4 [Both] Vendor / Procurement Owner tulee käynnistää toimittajan, henkilötietojen käsittelijän, alikäsittelijän tai ulkoistetun palveluntarjoajan korjaavat toimenpiteet REG08:n ja REG12:n kautta viiden työpäivän kuluessa, kun kolmas osapuoli ei täytä sovittuja poikkeama-, loukkaus-, näyttö- tai raportointivelvoitteita.

10.1.5 [Conditional] Top Management tulee katselmoida olennaiset tai toistuvat PII15-FS-poikkeamat seuraavassa suunnitellussa johdon katselmoinnissa, ja päätökset sekä vaaditut toimet säilytetään REG12:ssa.

10.1.6 [All] Privacy Lead / PIMS Manager tulee käynnistää korjaava koulutus REG11:ssä 30 kalenteripäivän kuluessa, kun politiikan poikkeama liittyy roolitietoisuuteen, myöhäiseen ilmoittamiseen, eskaloinnin epäonnistumiseen, näytön käsittelyn epäonnistumiseen tai viestinnän epäonnistumiseen.

## 11. Katselmointi ja ylläpito

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

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

11.1.3 [Conditional] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka 30 kalenteripäivän kuluessa siitä, kun se saa tiedon olennaisesta muutoksesta oikeudellisiin, toimialakohtaisiin, asiakas-, sopimus-, henkilötietojen käsittelijä-, alikäsittelijä-, raportointimalli-, raportointiaikataulu- tai siirtoon liittyviin poikkeamaraportointivaatimuksiin, ja katselmointinäyttö säilytetään 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-sisäisen auditointiohjelman kautta, ja auditointihavainnot sekä korjaavat toimenpiteet säilytetään REG12:ssa.

11.1.5 [Conditional] Top Management tulee katselmoida poikkeamatrendit, merkittävät loukkaukset, raportoinnin suorituskyky, erääntyneet korjaavat toimenpiteet ja politiikan vaikuttavuus suunnitellussa johdon katselmoinnissa, ja tuotokset säilytetään REG12:ssa.

11.1.6 [Conditional] Privacy Lead / PIMS Manager tulee katselmoida PII15-FS:n ja PII15:n välinen korvaussuhde vähintään vuosittain ja jokaisen PIMS-soveltamisalan muutoksen jälkeen varmistaakseen, ettei molempia politiikkoja toteuteta samassa finanssialan soveltamisalassa, ja katselmointinäyttö säilytetään REG03:ssa ja REG12:ssa.

## 12. Liittyvät politiikat

### 12.1 Tämä politiikka tulee lukea yhdessä seuraavien kanssa:

12.1.1 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.1.2 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka

12.1.3 PII03 - Henkilötietojen käsittelytoimien luetteloa ja oikeusperustetta koskeva politiikka

12.1.4 PII04 - Tietosuojaselostetta ja läpinäkyvyyttä koskeva politiikka

12.1.5 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.1.6 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.1.7 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.1.8 PII10 - Henkilötietojen säilytys-, poisto- ja hävityspolitiikka

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

12.1.10 PII13 - Henkilötietojen kansainvälisten siirtojen politiikka

12.1.11 PII14 - Henkilötietojen tietoturva- ja pääsynhallintapolitiikka

12.1.12 PII16 - Tietosuojakoulutuksen, tietoisuuden ja pätevyyden politiikka

12.1.13 PII17 - PIMS-dokumentoidun tiedon ja näytönhallinnan politiikka

12.1.14 PII18 - PIMS-seuranta-, auditointi- ja parantamispolitiikka

12.1.15 PII23 - Pilvipalvelujen henkilötietojen käsittelijäpolitiikka, kun finanssialan pilvipalvelujen käsittelijävelvoitteet kuuluvat soveltamisalaan

12.2 PII15 - henkilötietopoikkeamien ja henkilötietojen tietoturvaloukkausten hallintapolitiikka on poikkeamien ja tietoturvaloukkausten peruspolitiikka. PII15-FS on PII15:n korvaava finanssialakohtainen variantti. PII15:tä ja PII15-FS:ää ei saa toteuttaa samanaikaisesti samalle

PIMS-soveltamisalalle, liiketoimintayksikölle, tuotteelle, asiakasympäristölle, säännellylle palvelulle tai näyttörajoille.

## 13. Viitestandardit ja viitekehykset

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].