					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: PII15-FS					Dokumendi pealkiri: **Finantssektori PII intsidentide ja rikkumiste haldamise poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard / õigusnorm	Punkt / kontrollimeede / artikkel	Applicability	Coverage Type	Kommentaar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS teabevahetus ja dokumenteeritud intsidenditõendid
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Tegevuslik ohje ning privaatsusriskide hindamise ja käsitlemise seos
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seire, hindamine, mittevastavus, parandusmeetmed ja täiustamine
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Intsidendihalduse kavandamine ja ettevalmistus PII töötlemiseks
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reageerimine infoturbeintsidentidele, mis hõlmavad PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Õiguslikud, seadusest tulenevad, regulatiivsed ja lepingulised nõuded ning kirjete kaitse
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Volitatud töötleja kliendileping ja kliendi kohustuste toetamine
GDPR	Article 5(2); Article 24	Controller	Supporting	Vastutus ja vastutava töötleja vastutusala
GDPR	Article 26	Joint Controller	Supporting	Kaasvastutavate töötlejate intsidendivastutuse koordineerimine
GDPR	Article 28	Both	Supporting	Volitatud töötleja abi ja volitatud töötleja lepingulised kohustused
GDPR	Article 32	Both	Supporting	Töötlemise turvalisus ja rikkumiste tuvastamise võimekus
GDPR	Article 33	Both	Primary	Isikuandmete rikkumisest teatamine

				ja rikkumise dokumenteerimine
GDPR	Article 34	Controller	Primary	Isikuandmete rikkumistest mõjutatud PII principal'idele teavitamine
GDPR	Article 39	Conditional	Supporting	DPO nõustamine, seire, koostöö ja kontaktpunkti tugi
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	ICT-seotud intsidentide haldamise protsess kohaldamisalasse kuuluvatele finantsüksustele
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	ICT-seotud intsidentide ja oluliste küberohtude klassifitseerimise kriteeriumid
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Suurte ICT-seotud intsidentide aruandlus ja olulistest küberohtudest teavitamine
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Aruandluse sisu, tähtajad, mallid ja protseduurid
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Olulistest intsidentidest teatamine, kui kohaldub
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Infoturbe ja privaatsuse vastavuse põhimõtted
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII intsidendile reageerimise vastutused ja sündmustest teatamine
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Intsidendi kavandamine, hindamine, reageerimine, õppetunnid ja tõendite kogumine

ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Intsidendihalduse protsessi elutsükkel
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Intsidendipoliitika, plaan, teadlikkus, testimine ja õppetunnid
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Tuvastamine, teavitamine, triaaž, analüüs, reageerimine ja aruandlustoimingud
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Avaliku pilve volitatud töötleja teavitamise ja rikkumiskirjete ootused

1. Kohaldamisala

1.1 Käesolev poliitika määrab nõuded PII intsidentide ja PII rikkumiste tuvastamiseks, neist teatamiseks, triaažiks, klassifitseerimiseks, hindamiseks, ohjeldamiseks, teavitamiseks, dokumenteerimiseks, sulgemiseks ja nendest tulenevaks parendamiseks finantssektori PIMS-i kohaldamisalades.

1.2 **Rakendusteade:** Käesolev poliitika on finantssektori asendusvariant poliitikale PII15. Seda ei tohi rakendada samaaegselt poliitikaga PII15 sama PIMS-i kohaldamisala, äriüksuse, toote, kliendikeskkonna, reguleeritud teenuse või tõendusmaterjali piiri suhtes. Organisatsioonid peavad sama kohaldamisala jaoks valima kas PII15 või PII15-FS, et vältida dubleerivaid intsidendihalduse kohustusi, dubleerivaid registreid ja dubleerivat audititõendite tööd.

1.3 Käesolevat poliitikat kohaldatakse järgmistele olukordadele:

1.3.1 organisatsioon tegutseb finantssektori kontekstis PII vastutava töötlejana;

1.3.2 organisatsioon tegutseb kaasvastutava töötlejana, kui on vaja koordineerida vastutust intsidendi või rikkumise eest;

1.3.3 organisatsioon tegutseb finantssektori klientide jaoks PII volitatud töötlejana;

1.3.4 organisatsioon tegutseb finantssektori klientide või eelnevate volitatud töötlejate jaoks alltöötlejana;

1.3.5 süsteemid, rakendused, teenused, protsessid, tarnijad, volitatud töötlejad, alltöötlejad ja kolmandad osapooled, kes töötlevad, säilitavad, edastavad, toetavad, pääsevad juurde või muul viisil mõjutavad PII-d finantssektori PIMS-i kohaldamisala piires.

1.4 Käesolevas poliitikas kasutatakse REG10 - PII intsidentide ja rikkumiste registrit peamise tõendusobjektina finantssektori PII intsidentide ja rikkumiste haldamisel.

1.5 Käesolevas poliitikas kasutatakse toetavaid tõendusobjekte järgmiselt:

1.5.1 REG01 PIMS-i kohaldamisala, asjakohaste huvitatud poolte, sektori, klientide, lepingulise ja aruandluskonteksti jaoks.

1.5.2 REG02 mõjutatud töötlemistoimingute, PII kategooriate, PII principal'i kategooriate, eesmärkide, süsteemide ja teenuste jaoks.

1.5.3 REG03 kohaldatavusavalduse ja kontrollimeetmete kohaldatavuse ajakohastuste jaoks, sealhulgas PII15 asendamine poliitikaga PII15-FS sama kohaldamisala suhtes.

1.5.4 REG04 privaatsusriski, DPIA, jääkriski ja riskikäsitluse seoste jaoks.

1.5.5 REG08 volitatud töötleja, alltöötleja, kliendi, tarnija ja kolmanda osapoole intsidendiliidese tõendusmaterjali jaoks.

1.5.6 REG09 rahvusvahelise edastuse seoste jaoks, kui intsident mõjutab piiriülest töötlemist.

1.5.7 REG11 koolituse, teadlikkuse ja intsidendile reageerimise pädevuse tõendusmaterjali jaoks.

1.5.8 REG12 auditi, mittevastavuse, parandusmeetmete, juhtkonna läbivaatamise ja täiustamise tõendusmaterjali jaoks.

1.6 Käesolev poliitika tugineb spetsialiseeritud kontrollimeetmete puhul seotud PIMS poliitikatele:

1.6.1 PII03 reguleerib töötlemisregistrit ja õigusliku aluse kirjeid.

1.6.2 PII04 reguleerib privaatsusteadet ja läbipaistvuse kontrollimeetmeid väljaspool rikkumisspetsiifilist teabevahetust.

1.6.3 PII06 reguleerib PII principal'i õiguste taotlusi, mis tekivad enne intsidenti, selle ajal või pärast seda.

1.6.4 PII07 reguleerib privaatsusriskide hindamise ja DPIA metoodikat.

1.6.5 PII08 reguleerib privaatsust kavandamisel ja vaikimisi andmekaitse kontrollimeetmeid.

1.6.6 PII10 reguleerib säilitamise, kustutamise ja kõrvaldamise kontrollimeetmeid.

1.6.7 PII12 reguleerib volitatud töötlejate, alltöötlejate, tarnijate ja kolmandate osapoolte privaatsussuhete kontrollimeetmeid.

1.6.8 PII13 reguleerib rahvusvahelisi PII edastusmehhanisme ja edastusriski kirjeid.

1.6.9 PII14 reguleerib ennetavaid ja tuvastavaid PII turbe- ja juurdepääsukontrolle.

1.6.10 PII16 reguleerib privaatsuskoolitust, teadlikkust ja pädevust.

1.6.11 PII17 reguleerib dokumenteeritud teabe ja tõendusmaterjali haldamist.

1.6.12 PII18 reguleerib seiret, siseauditit, juhtkonna läbivaatamist, mittevastavust, parandusmeetmeid ja pidevat täiustamist.

1.6.13 PII23 reguleerib pilve PII volitatud töötleja kontrollimeetmeid, kui pilve volitatud töötleja kohustused kuuluvad kohaldamisalasse.

1.7 Käesolevas poliitikas:

1.7.1 „PII intsident“ tähendab kahtlustatavat või kinnitatud sündmust, mis on mõjutanud, võib olla mõjutanud või võiks mõistlikult mõjutada PII konfidentsiaalsust, terviklust, käideldavust, seaduslikku töötlemist või volitatud käitlemist.

1.7.2 „PII rikkumine“ tähendab kinnitatud PII intsidenti, mis hõlmab PII volitamata, õigusvastast, juhuslikku või ettekavatsemata hävitamist, kaotsiminekut, muutmist, avalikustamist, juurdepääsu, kättesaamatust või kompromiteerimist.

1.7.3 „Finantssektori PII intsident“ tähendab PII intsidenti, mis mõjutab, võib mõjutada või on mõistlikult seotud reguleeritud finantsteenuste, finantssektori klientide, finantssektori vastaspoolte, finantstehingute, finantstoimingute või finantssektori PII töötlemisega.

1.7.4 „Suur finantssektori intsident“ tähendab finantssektori PII intsidenti või seotud ICT intsidenti, mis vastab dokumenteeritud olulisuse või aruandluse kriteeriumidele registris REG10.

1.7.5 „Oluline küberoht“ tähendab registris REG10 kirjendatud küberohtu, mis võib oluliselt mõjutada kohaldamisalasse kuuluvaid finantssektori teenuseid, PII töötlemist, kliente, vastaspooli või toiminguid.

1.7.6 „Rikkumise hindamine“ tähendab dokumenteeritud hindamist selle kohta, kas PII intsident on PII rikkumine, milline PII ja millised PII principal'id on mõjutatud, millised riskid võivad tekkida, milliseid teavitusi või teabevahetust on vaja ning milliseid parandusmeetmeid tuleb võtta.

1.7.7 „Teadlikuks saamine“ tähendab hetke, mil organisatsioonil on mõistlik kindlus, et turbe- või privaatsusintsident on toimunud ning PII on või võib olla kompromiteeritud.

1.7.8 „Suure mõjuga finantssektori PII intsident“ tähendab PII intsidenti, mis hõlmab kõrge riskiga töötlemist, eriliiki või väga tundlikku PII-d, suuremahulist PII-d, haavatavaid isikuid, reguleeritud kliente, olulist teenusekatkestust, finantssektori vastaspooli, finantstehinguid, mitme jurisdiktsiooni mõju, privilegeeritud juurdepääsu kompromiteerimist, avalikku kokkupuudet, lunavara, teenuse kättesaamatust või olulist operatiivset, kliendi-, finants- või mainealast mõju.

1.7.9 „Oluline intsidendimuudatus“ tähendab uut või muutunud teavet, mis mõjutab intsidendi ulatust, raskusastet, PII kategooriaid, PII principal'i mõju, teenuse mõju, finantssektori klassifikatsiooni, teavitamisotsust, kliendimõju, algpõhjust, ohjeldamist, taastamist, parandusmeedet või välise aruandluse kohustusi.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et PII intsidente ja rikkumisi finantssektori kontekstides käsitletakse järjepidevalt, viivitamata, õiguspäraselt, turvaliselt ja auditiks valmis tõendusmaterjaliga.

2.2 Käesolev poliitika toetab vastutust, nõudes finantssektori PII intsidentide ja rikkumiste kirjendamist registris REG10 ning nende seostamist mõjutatud töötlemiskirjete, privaatsusriskide, volitatud töötlejate ja alltöötlejate suhete, edastuskirjete, parandusmeetmete, koolituskirjete, finantssektori aruandlusotsuste ja juhtkonna läbivaatamise tõendusmaterjaliga, kui see on käivitatud.

2.3 Käesolev poliitika tagab, et vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kohustusi käsitletakse eraldi kohaldatavusreeglite kaudu, säilitades samal ajal ühe integreeritud finantssektori intsidentide ja rikkumiste tõendusmudeli.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 tagada, et kahtlustatavatest finantssektori PII intsidentidest teatatakse ja need kirjendatakse viivitamata;

3.1.2 tagada, et finantssektori PII intsidente hinnatakse esmaselt ja klassifitseeritakse järjepidevate privaatsus-, turbe-, operatiivsete ja sektoripõhiste kriteeriumide alusel;

3.1.3 tagada, et rikkumise hindamisel võetakse arvesse mõjutatud PII-d, PII principal'e, süsteeme, teenuseid, töötlemistoiminguid, volitatud töötlejaid, alltöötlejaid, edastusi, riske, kliente, vastaspooli ja parandusmeetmeid;

3.1.4 tagada, et vastutava töötleja teavitamisotsused ja PII principal'idele suunatud teavitamisotsused dokumenteeritakse;

3.1.5 tagada, et volitatud töötleja ja alltöötleja rikkumisteavitused klientidele või eelnevatele pooltele tehakse põhjendamatu viivituseta ja kooskõlas kohaldatavate lepingutega;

3.1.6 tagada, et finantssektori aruandluse käivitajad hinnatakse, dokumenteeritakse ja jälgitakse, kui see on kohaldatav;

3.1.7 tagada, et intsidendi käsitlemise ajal säilitatakse ja kaitstakse tõendusmaterjali;

3.1.8 tagada, et ohjeldamist, kõrvaldamist, taastamist ja valideerimist jälgitakse registri REG10 kaudu;

3.1.9 tagada, et olulised küberohud ja suured finantssektori intsidendid suunatakse asjakohastesse otsustus- ja aruandlustöövoogudesse;

3.1.10 tagada, et intsidendist saadud õppetunnid viivad parandusmeetmete, koolituse, kontrollimeetmete täiustamise ja juhtkonna läbivaatamiseni;

3.1.11 tagada, et intsidendi- ja rikkumiskirjed on vajaduse korral kättesaadavad auditi, juhtkonna läbivaatamise, kliendikindluse ja regulatiivse läbivaatamise jaoks;

3.1.12 tagada, et PII15-FS asendab PII15 sama finantssektori kohaldamisala suhtes ega dubleeri PII15 tõendusmaterjali tööd.

4. Poliitika seisukohad

4.1 Variandi aktiveerimine, valmisolek ja vastuvõtt

4.1.1 [Conditional] Privacy Lead / PIMS Manager peab dokumenteerima PII15-FS aktiveerimise registrites REG01 ja REG03 enne käesoleva poliitika kasutamist finantssektori PIMS-i kohaldamisalas.

4.1.2 [Conditional] Privacy Lead / PIMS Manager peab dokumenteerima registrites REG03 ja REG12, et PII15 ei ole sama finantssektori PIMS-i kohaldamisala suhtes samaaegselt rakendatud, enne kui PII15-FS heaks kiidetakse.

4.1.3 [All] Incident Response Coordinator peab kirjendama iga teatatud või tuvastatud kahtlustatava finantssektori PII intsidendi registris REG10 ühe tööpäeva jooksul alates kättesaamisest või varem, kui kohaldatav teavitamise, kliendi või aruandluse tähtaeg võib käivituda.

4.1.4 [Conditional] Privacy Lead / PIMS Manager peab haldama finantssektori PII intsidentide ja rikkumiste käsitlemise kriteeriume registris REG10 vähemalt kord aastas ning pärast iga olulist muudatust PIMS-i kohaldamisalas, õiguslikus kontekstis, kliendikohustustes, lepingulistes kohustustes, sektoripõhises aruandluskontekstis või kõrge riskiga töötlemises.

4.1.5 [Both] Information Security Lead peab kinnitama intsidendi tõendusmaterjali säilitamise nõuded registris REG10 24 tunni jooksul pärast seda, kui kahtlustatav intsident mõjutab süsteemi, teenust või rakendust, mis töötleb PII-d.

4.1.6 [Conditional] Vendor / Procurement Owner peab enne kaasamist ja vähemalt kord aastas hoidma registris REG08 ajakohasena finantssektori kolmandate osapoolte intsidendikontaktide ja tõendusmaterjali suunamise nõuded kohaldamisalasse kuuluvate volitatud töötlejate, alltöötlejate, tarnijate ja sisseostetud aruandlusteenuse osutajate jaoks.

4.2 Klassifitseerimine ja rikkumise hindamine

4.2.1 [All] Incident Response Coordinator peab klassifitseerima iga REG10 kande 24 tunni jooksul pärast vastuvõttu kas mitte-PII sündmuseks, kahtlustatavaks PII intsidendiks, kinnitatud PII intsidendiks, kinnitatud PII rikkumiseks, finantssektori PII intsidendiks, suureks finantssektori intsidendiks, oluliseks küberohuks või klassifitseerimist ootavaks kandeks.

4.2.2 [Conditional] Information Security Lead peab hindama mõjutatud teenuseid, kliente, vastaspooli, tehinguid, teenuse seisakut, geograafilist ulatust, andmekadu, teenuse kriitilisust ja majanduslikku mõju registris REG10, kui PII intsident võib mõjutada finantssektori teenuseid või toiminguid.

4.2.3 [Both] Privacy Lead / PIMS Manager peab tuvastama mõjutatud töötlemistoimingu, PII kategooriad, PII principal'i kategooriad, süsteemid, volitatud töötlejad, alltöötlejad, edastuskohad ja privaatsusriskid registrites REG02, REG04, REG08, REG09 ja REG10 enne rikkumisest teavitamise otsuse lõplikku vormistamist.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor peab hindama riski mõjutatud PII principal'idele iga kinnitatud või mõistlikult kahtlustatava PII rikkumise korral ning kirjendama teavitamissoovituse, riski põhjenduse ja nõuande registris REG10 enne välise teavitamisotsuse tegemist.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager peab kirjendama kaasvastutavate töötlejate intsidendivastutuse jaotuse registrites REG08 ja REG10 24 tunni jooksul pärast jagatud vastutuse tuvastamist kahtlustatava või kinnitatud PII rikkumise puhul.

4.2.6 [Processor] Privacy Lead / PIMS Manager peab hindama kliendi juhiseid, lepingulisi teavitamiskohustusi ja koostöökohustusi registrites REG08 ja REG10 24 tunni jooksul pärast seda, kui kahtlustatav või kinnitatud PII rikkumine mõjutab volitatud töötlejana tehtavat töötlemist.

4.2.7 [Subprocessor] Vendor / Procurement Owner peab tuvastama ülespoole suunatud teavitusahela ja nõutava tõendusmaterjali suunamise registrites REG08 ja REG10 24 tunni jooksul pärast seda, kui kahtlustatav või kinnitatud PII intsident mõjutab alltöötlejana tehtavat töötlemist.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Erandid

9.1.1 [All] Privacy Lead / PIMS Manager peab kirjendama iga erandi käesolevast poliitikast registris REG12 enne rakendamist või 24 tunni jooksul pärast erakorralist tegevust, kui eelnev heakskiit ei olnud teostatav.

9.1.2 [Conditional] Top Management peab enne intsidendi sulgemist heaks kiitma iga erandi, mis oluliselt mõjutab rikkumisest teavitamise ajastust, finantssektori aruandluse ajastust, avalikku teabevahetust, kliendikohustust, tõendusmaterjali säilitamist või PII principal'i riski, ning heakskiidu tõendusmaterjal tuleb säilitada registrites REG10 ja REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor peab enne intsidendi sulgemist dokumenteerima nõuande iga viivitatud teavituse, teavitamata jätmise otsuse, aruandluserandi või erakorralise teabevahetuse lähenemisviisi kohta ning nõuanne tuleb säilitada registris REG10.

9.1.4 [Both] Vendor / Procurement Owner peab kirjendama tarnija, volitatud töötleja, alltöötleja, kliendi või sisseostetud teenuseosutaja erandid, mis mõjutavad finantssektori intsidendile reageerimist, registrites REG08 ja REG12 viie tööpäeva jooksul pärast erandi tuvastamist.

9.1.5 [All] Privacy Lead / PIMS Manager peab avatud erandid käesolevast poliitikast läbi vaatama vähemalt kord kuus kuni sulgemiseni ning läbivaatamise staatus tuleb säilitada registris REG12.

10. Järgimise tagamine

10.1.1 [All] Process Owner / Business Owner peab eskaleerima kahtlustatavast finantssektori PII intsidendist teatamata jätmise, tõendusmaterjali säilitamata jätmise, määratud tegevuste täitmata jätmise või rikkumise hindamisel koostööst keeldumise rollile Privacy Lead / PIMS Manager kahe tööpäeva jooksul pärast avastamist ning tõendusmaterjal tuleb säilitada registris REG12.

10.1.2 [Both] Incident Response Coordinator peab eskaleerima hilise teatamise, tegemata klassifitseerimise, puuduva tõendusmaterjali, tegemata eskalatsiooni või tähtaja ületanud ohjeldamistegevuse rollile Privacy Lead / PIMS Manager ühe tööpäeva jooksul pärast probleemi tuvastamist ning tõendusmaterjal tuleb säilitada registrites REG10 ja REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager peab kirjendama REG12 mittevastavuse, kui käesoleva poliitika rikkumine mõjutab intsidendi vastuvõttu, triaaži, ohjeldamist, teavitamist, aruandlust, tõendusmaterjali terviklust, teabevahetust või parandusmeedet.

10.1.4 [Both] Vendor / Procurement Owner peab algatama tarnija, volitatud töötleja, alltöötleja või sisseostetud teenuseosutaja parandusmeetmed registrite REG08 ja REG12 kaudu viie tööpäeva jooksul, kui kolmas osapool ei täida kokkulepitud intsidendi-, rikkumise-, tõendusmaterjali- või aruandluskohustusi.

10.1.5 [Conditional] Top Management peab olulised või korduvad PII15-FS mittevastavused läbi vaatama järgmisel kavandatud juhtkonna läbivaatamisel ning otsused ja nõutavad tegevused tuleb säilitada registris REG12.

10.1.6 [All] Privacy Lead / PIMS Manager peab käivitama parandusõppe registris REG11 30 kalendripäeva jooksul, kui poliitika mittevastavus hõlmab rolliteadlikkust, hilist teatamist, eskaleerimise ebaõnnestumist, tõendusmaterjali käitlemise ebaõnnestumist või teabevahetuse ebaõnnestumist.

11. Läbivaatamine ja ajakohastamine

11.1.1 [Conditional] Privacy Lead / PIMS Manager peab käesoleva poliitika läbi vaatama vähemalt kord aastas ning kirjendama läbivaatamise tulemuse, nõutavad muudatused ja heakskiidu staatuse registris REG12.

11.1.2 [Conditional] Incident Response Coordinator peab käivitama käesoleva poliitika intsidendijärgse läbivaatamise 30 kalendripäeva jooksul pärast iga suure mõjuga finantssektori

PII intsidendi, kinnitatud PII rikkumise, suure finantssektori intsidendi või olulise küberohu sulgemist ning läbivaatamise tõendusmaterjal tuleb säilitada registrites REG10 ja REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager peab käesoleva poliitika läbi vaatama 30 kalendripäeva jooksul pärast seda, kui saab teadlikuks olulisest muudatusest õiguslikes, sektoripõhistes, kliendi-, lepingulistes, volitatud töötleja, alltöötleja, aruandlusmalli, aruandlustähtaja või edastusega seotud intsidendiaruandluse nõuetes, ning läbivaatamise tõendusmaterjal tuleb säilitada registrites REG01, REG08, REG09 ja REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer peab käesoleva poliitika rakendamist läbi vaatama vähemalt kord aastas PIMS siseauditi programmi kaudu ning auditileiud ja parandusmeetmed tuleb säilitada registris REG12.

11.1.5 [Conditional] Top Management peab kavandatud juhtkonna läbivaatamisel läbi vaatama intsidendisuundumused, olulised rikkumised, aruandluse tulemuslikkuse, tähtaja ületanud parandusmeetmed ja poliitika tõhususe ning väljundid tuleb säilitada registris REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager peab vähemalt kord aastas ja pärast iga PIMS-i kohaldamisala muudatust läbi vaatama asendussuhte PII15-FS ja PII15 vahel, et kontrollida, et mõlemat poliitikat ei rakendata sama finantssektori kohaldamisala suhtes, ning läbivaatamise tõendusmaterjal tuleb säilitada registrites REG03 ja REG12.

12. Seotud poliitikad

12.1 Käesolevat poliitikat tuleb lugeda koos järgmiste poliitikatega:

12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika

12.3 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika

12.4 PII03 - PII töötlemisregistri ja õigusliku aluse poliitika

12.5 PII04 - Privaatsusteate ja läbipaistvuse poliitika

12.6 PII06 - PII principal'i õiguste haldamise poliitika

12.7 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

12.8 PII08 - Privaatsus kavandamisel ja vaikimisi andmekaitse poliitika

12.9 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.10 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsushalduse poliitika

12.11 PII13 - Rahvusvahelise PII edastuse poliitika

12.12 PII14 - PII turbe- ja juurdepääsukontrolli poliitika

12.13 PII16 - Privaatsuskoolituse, teadlikkuse ja pädevuse poliitika

12.14 PII17 - PIMS dokumenteeritud teabe ja tõendusmaterjali haldamise poliitika

12.15 PII18 - PIMS seire, auditi ja täiustamise poliitika

12.16 PII23 - Pilve PII volitatud töötleja poliitika, kui finantssektori pilve volitatud töötleja kohustused kuuluvad kohaldamisalasse

12.17 PII15 - PII intsidentide ja rikkumiste haldamise poliitika on intsidendi- ja rikkumishalduse baaspoliitika. PII15-FS on finantssektori asendusvariant poliitikale PII15. PII15 ja PII15-FS ei tohi olla samaaegselt rakendatud sama PIMS-i kohaldamisala, äriüksuse, toote, kliendikeskkonna, reguleeritud teenuse või tõendusmaterjali piiri suhtes.

13. Viitestandardid ja raamistikud

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].