					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: PII17					Dokumendi pealkiri: **PIMS-i dokumenteeritud teabe ja tõendusmaterjali 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 / kontroll / artikkel	Kohaldatavus	Katvuse tüüp	Kommentaar
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA dokumenteeritud teave
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS-i dokumenteeritud teave
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Tegevustõendite ohje
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Seire tõendusmaterjal
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Audititõendus
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Juhtkonna läbivaatamise tõendusmaterjal
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Mittevastavuse ja parandusmeetmete tõendusmaterjal
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Vastutava töötleja töötlemiskirjed
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Volitatud töötleja lepingu ja juhiste tõendusmaterjal
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Kirjete kaitse
GDPR	Article 5(2)	Controller	Supporting	Vastutuse tõendusmaterjal
GDPR	Article 24	Controller	Supporting	Vastutava töötleja meetmed ja tõendusmaterjal
GDPR	Article 28	Both	Supporting	Volitatud töötleja dokumentatsioon
GDPR	Article 30	Both	Supporting	Töötlemiskirjed
GDPR	Article 32	Both	Supporting	Tõendusmaterjali kaitse
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privaatsusnõuetele vastavuse tõendusmaterjal
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Kirjete kaitse

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Dokumenteeritud teabe ohje
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Kirjete kaitse
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Privaatsuse ja PII kaitse

1. Kohaldamisala

1.1 See poliitika määrab kohustuslikud nõuded PIMS-i dokumenteeritud teabe loomisele, kinnitamisele, versioonimisele, kaitsmisele, säilitamisele, kättesaamisele, tõlkimisele, tagasivõtmisele ja tõendamisele.

1.2 Seda poliitikat kohaldatakse PIMS-i poliitikatele, registritele, dokumenteeritud kinnitustele, tõendusmaterjali kirjetele, audititõendusele, juhtkonna läbivaatamise kirjetele, parandusmeetmete tõendusmaterjalile ning kontrollitud tõlgetele, mida kasutatakse PIMS-i nõuetele vastavuse tõendamiseks.

1.3 Seda poliitikat kohaldatakse vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kontekstides.

1.4 See poliitika ei loo eraldi dokumendihalduse registrit. Dokumenteeritud teabe ohje tõendusmaterjali hallatakse kanooniliste PIMS-i tõendusobjektide REG01 kuni REG12 kaudu, kusjuures REG03 ja REG12 kasutatakse kontrollimeetmete kohaldatavuse, auditi, mittevastavuse, parandusmeetmete ja täiustamise tõendusmaterjali jaoks.

2. Eesmärk

2.1 Selle poliitika eesmärk on tagada, et PIMS-i dokumenteeritud teave oleks täpne, ohjatud, volitatud kasutajatele kättesaadav, kaitstud loata muutmise või avalikustamise eest, säilitatud auditeeritavuse tagamiseks ning vananemisel tagasi võetud.

2.2 See poliitika toetab valmisolekut sertifitseerimiseks, tagades, et PIMS-i nõuetele vastavuse tõendamiseks vajalikku tõendusmaterjali saab leida, kontrollida, kätte saada ning siduda kohaldatavate poliitikate, kontrollimeetmete, töötlemistoimingute, riskide, auditite ja parandusmeetmetega.

3. Eesmärgid

3.1 Selle poliitika eesmärgid on:

3.1.1 määratleda PIMS-i dokumenteeritud teabe ohje nõuded;

3.1.2 säilitada tõendusmaterjali terviklus REG01 kuni REG12 lõikes;

3.1.3 tagada poliitika ja tõendusmaterjali kinnitamise jälgitavus;

3.1.4 tagada versiooniajaloo ja tagasivõtmise otsuste dokumenteerimine;

3.1.5 siduda PIMS-i tõendusmaterjal kohaldatavusavalduse ja poliitikate vastendustega;

3.1.6 ohjata juurdepääsu PIMS-i dokumentidele ja tõendusmaterjali kirjetele;

3.1.7 toetada mitmekeelset poliitika ja tõendusmaterjali versioonihaldust;

3.1.8 võimaldada audititõenduse õigeaegset kättesaamist;

3.1.9 vältida ebavajalikku dokumendihalduse bürokraatiat;

3.1.10 säilitada auditiks valmis kirjed sertifitseerimise, klientidele kindluse andmise ja pideva täiustamise jaoks.

4. Poliitika sätted

4.1 PIMS-i dokumenteeritud teabe ohje

4.1.1 [All] Privacy Lead / PIMS Manager peab enne PIMS-i esmast avaldamist ja seejärel kord kvartalis pidama PIMS-i dokumenteeritud teabe indeksit REG12-s.

4.1.2 [All] Process Owner / Business Owner peab enne töötlemistoimingu algust ja seejärel igal aastal tuvastama REG02-s dokumenteeritud teabe, mida on vaja iga tema vastutusalas oleva PII töötlemistoimingu jaoks.

4.1.3 [All] Privacy Lead / PIMS Manager peab enne iga poliitika väljalaset ja 15 tööpäeva jooksul pärast iga olulist kontrollimeetme kohaldatavuse muudatust siduma kohaldatavad PIMS-i poliitikad, kontrollimeetmed ja tõenduskohustused REG03-ga.

4.1.4 [All] Privacy Lead / PIMS Manager peab enne kategooria kasutuselevõttu määrama REG12-s igale PIMS-i dokumenteeritud teabe kategooriale juurdepääsutaseme ja tõendusmaterjali tundlikkuse klassifikatsiooni.

4.2 Loomine, kinnitamine, versioonimine ja avaldamine

4.2.1 [All] Privacy Lead / PIMS Manager peab enne PIMS-i dokumenteeritud teabe avaldamist määrama REG12-s dokumendi identifikaatori, omaniku, versiooninumbri, kinnitamise staatuse, jõustumiskuupäeva ja läbivaatamise kuupäeva.

4.2.2 [All] Top Management peab enne avaldamist kinnitama REG12-s PIMS-i põhipoliitikad ja olulised poliitikamuudatused.

4.2.3 [All] Privacy Lead / PIMS Manager peab enne operatiivset kasutamist kinnitama REG12-s PIMS-i tõendusmaterjali mallid või registritesse põimitud jaotised.

4.2.4 [All] Privacy Lead / PIMS Manager peab enne ajakohastatud PIMS-i dokumenteeritud teabe väljalaskmist registreerima REG12-s versiooniajaloo ja muudatuse põhjenduse.

4.2.5 [All] Privacy Lead / PIMS Manager peab 30 päeva jooksul pärast avaldamist registreerima REG11-s kinnitatud PIMS-i dokumenteeritud teabe muudatustest teavitamise.

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

9. Erandid

9.1.1 [All] Process Owner / Business Owner peab enne sellest poliitikast kõrvalekaldumist taotlema REG12-s dokumenteeritud teabe või tõendusmaterjali ohje erandeid.

9.1.2 [All] Privacy Lead / PIMS Manager peab hindama iga dokumenteeritud teabe või tõendusmaterjali ohje erandit REG12-s 10 tööpäeva jooksul pärast taotlust.

9.1.3 [All] Data Protection Officer / Privacy Advisor peab enne iga erandi kinnitamist, mis hõlmab PII tõendusmaterjali avalikustamist, tõlkelahknevust, säilitamiskonflikti või audititõenduse piirangut, registreerima REG12-s nõuande.

9.1.4 [All] Top Management peab enne erandi jõustumist kinnitama REG12-s dokumenteeritud teabe erandid, mis ületavad 30 päeva või mõjutavad sertifitseerimist, suure riskiga töötlemist või välist kindlustunnet.

9.1.5 [All] Privacy Lead / PIMS Manager peab iga kinnitatud dokumenteeritud teabe või tõendusmaterjali ohje erandi jaoks määrama REG12-s aegumiskuupäeva, mis ei ületa 90 päeva.

9.1.6 [All] Privacy Lead / PIMS Manager peab iga dokumenteeritud teabe või tõendusmaterjali ohje erandi sulgema või uuesti hindama REG12-s viie tööpäeva jooksul pärast aegumist.

10. Jõustamine

10.1.1 [All] Privacy Lead / PIMS Manager peab puuduva, ebatäpse, ohjamata, vananenud või kättesaamatu PIMS-i dokumenteeritud teabe registreerima REG12-s mittevastavusena viie tööpäeva jooksul pärast tuvastamist.

10.1.2 [All] Privacy Lead / PIMS Manager peab takistama PIMS-i dokumenteeritud teabe avaldamist, kui nõutav kinnitus, versioon, omanik või jõustumiskuupäeva tõendusmaterjal puudub REG12-st.

10.1.3 [All] Process Owner / Business Owner peab takistama töötlemise tõendusmaterjali esitamist auditiks, kui nõutav omanik, kuupäev, staatus või kinnituse tõendusmaterjal puudub REG02-st.

10.1.4 [All] System Owner / Application Owner peab eemaldama loata juurdepääsu PIMS-i dokumenteeritud teabe hoidlatele ja registreerima eemaldamise REG12-s ühe tööpäeva jooksul pärast tuvastamist.

10.1.5 [All] Internal Audit / Compliance Reviewer peab dokumenteeritud teabe mittevastavuste parandusmeetmete tõhusust kontrollima REG12-s järgmisel kavandatud auditil või 60 päeva jooksul pärast sulgemist, olenevalt sellest, kumb toimub varem.

11. Läbivaatamine ja ajakohastamine

11.1.1 [All] Privacy Lead / PIMS Manager peab selle poliitika läbi vaatama igal aastal ja 30 päeva jooksul pärast olulist muudatust PIMS-i dokumenteeritud teabe nõuetes.

11.1.2 [All] Privacy Lead / PIMS Manager peab selle poliitika läbi vaatama 30 päeva jooksul pärast olulist auditileidu, sertifitseerimise mittevastavust, hoidlaplatvormi muudatust või mitmekeelse avaldamise protsessi muudatust.

11.1.3 [All] Data Protection Officer / Privacy Advisor peab enne kinnitamist läbi vaatama REG12-s selle poliitika privaatsuse seisukohast olulised muudatused.

11.1.4 [All] Top Management peab enne avaldamist kinnitama REG12-s selle poliitika olulised muudatused.

11.1.5 [All] Privacy Lead / PIMS Manager peab 30 päeva jooksul pärast avaldamist registreerima REG11-s selle poliitika kinnitatud muudatustest teavitamise.

12. Seotud poliitikad

12.1 Seda poliitikat toetavad järgmised seotud poliitikad:

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 PII05 - Nõusoleku ja eelistuste haldamise poliitika

12.7 PII06 - Isikuandmesubjekti õiguste haldamise poliitika

12.8 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

12.9 PII08 - Lõimitud ja vaikimisi privaatsuse poliitika

12.10 PII09 - PII kogumise, kasutamise, avalikustamise ja jagamise poliitika

12.11 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika

12.12 PII11 - PII täpsuse ja kvaliteedi poliitika

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

12.14 PII13 - Rahvusvahelise PII edastamise poliitika

12.15 PII14 - PII turbe ja juurdepääsukontrolli poliitika

12.16 PII15 - PII intsidentide ja rikkumiste haldamise poliitika

12.17 PII16 - Privaatsuskoolituse, teadlikkuse ja pädevuse poliitika

12.18 PII18 - PIMS-i seire, auditi ja täiustamise poliitika

13. Viitestandardid ja raamistikud

13.1 See poliitika on vastendatud järgmiste standardite ja õigusnormidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning tuvastab sisemised punktid, mis neid rakendavad või toetavad.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Vastendatud PIMS-i kohaldatavusavalduse, kontrollimeetmete kohaldatavuse kirjete ning poliitika ja tõendusmaterjali seoste haldamisega. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Vastendatud dokumenteeritud teabe tuvastamise, kinnitamise, versioonihalduse, juurdepääsu, kättesaamise, säilitamise, tagasivõtmise, tõlkeversiooni seose

ja säilitamise metaandmetega. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Vastendatud töötlemiskirjete, tõendusmaterjali mallide, tegevustõendite kvaliteedi ja väliselt esitatud tõendusmaterjaliga seotud tegevuse planeerimise ja ohjega. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Vastendatud mõõtmise, kättesaamise toimivuse, tõendusmaterjali puudujääkide, tõlkelahknevuste ja hoidlate juurdepääsuõiguste läbivaatamise lõpuleviimise dokumenteeritud tõendusmaterjali haldamisega. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Vastendatud audititõenduse kättesaamise, auditi valimite, audititõenduse jälgitavuse ning dokumenteeritud teabe ohjega seotud auditileidudega. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Vastendatud juhtkonna läbivaatamise tõendusmaterjali, dokumenteeritud teabe ohje käsitlemisega juhtkonna läbivaatamisel ning Top Management poolt tõendusmaterjali ohje toimivuse läbivaatamisega. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Vastendatud dokumenteeritud teabe mittevastavuste, parandusmeetmete, erandite käsitlemise, sulgemise ja tõhususe kontrollimisega. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Vastendatud vastutava töötleja töötlemiskirjete, vastutuse kirjete, töötlemise tõendusmaterjali kvaliteedi ning vastutava töötleja kohustusi toetava tõendusmaterjali säilitamisega. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Vastendatud volitatud töötleja lepingu, kliendi juhiste, väliselt esitatud tõendusmaterjali ja volitatud töötleja suhte tõendusmaterjali ohjega. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Vastendatud PIMS-i kirjete kaitsmisega kaotsimineku, loata muutmise, loata juurdepääsu, loata väljastamise ja nõuetele mittevastava kõrvaldamise eest. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Vastendatud vastutuse tõendusmaterjali, tõendusmaterjali jälgitavuse, tõendusmaterjali kättesaamise, mittevastavuste kirjete ja vastavust tõendavate auditiks valmis kirjetega. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Vastendatud vastutava töötleja juhtimise tõendusmaterjali, kinnituste kirjete, poliitika ohje, vastutusmeetmete, dokumenteeritud läbivaatamise ja Top Management järelevalvega. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Vastendatud volitatud töötleja ja alltöötleja dokumentatsiooni, kliendi juhiste tõendusmaterjali, väliselt esitatud protsessitõendite ning tõendusmaterjali avalikustamise ohjega. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Vastendatud töötlemiskirjete tõendusmaterjali, tõendusmaterjali kvaliteedinõuete, töötlemistoimingu viidete ning töötlemise tõendusmaterjali omaniku ja staatuse metaandmetega. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Vastendatud tõendusmaterjali hoidlate kaitse, juurdepääsupiirangute, juurdepääsukinnituste, hoidla kaitse läbivaatuse ja loata juurdepääsu eemaldamisega. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Vastendatud privaatsusnõuetele vastavuse tõendusmaterjali, audititõenduse kättesaamise, tõendusmaterjali jälgitavuse, sõltumatu läbivaatamise toe ja parandusmeetmete tõendusmaterjaliga. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Vastendatud PII-ga seotud kirjete kaitse, kirjete säilitamise ning tõendusmaterjali hoidlate juurdepääsu- ja kustutuskontrollidega. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Vastendatud dokumenteeritud teabe tuvastamise, kinnitamise, kättesaadavuse, kaitse, versioonihalduse, säilitamise, kõrvaldamise ja väliselt nõutava dokumenteeritud teabe ohjega. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Vastendatud PIMS-i kirjete kaitsmisega kaotsimineku, hävitamise, võltsimise, loata juurdepääsu, loata väljastamise ja nõuetele mittevastava kõrvaldamise eest. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Vastendatud privaatsuse ja PII kaitsmisega dokumenteeritud teabes, tõendusmaterjali hoidlates, avalikustamistel ja juurdepääsukontrolliga kirjete puhul. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].