					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: PII16					Dokumendi pealkiri: **Privaatsuskoolituse, teadlikkuse ja pädevuse 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	Kohaldatavus	Katvuse tüüp	Kommentaar
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Pädevus ja teadlikkus
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Teabevahetus ja dokumenteeritud tõendusmaterjal
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Tegevuse ohje, mõõtmine ja täiustamine
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	PII töötlemise alane teadlikkus, haridus ja koolitus
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Vastutus, volitatud töötlejate juhtimine, turvalisus ja andmekaitseametniku ülesanded
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Pädevus, teadlikkus ja koolitus
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Teadlikkuse, hariduse ja koolituse suunised
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Infoturve ja privaatsuse vastavus

1. Kohaldamisala

1.1 Käesolev poliitika määratleb organisatsiooni nõuded privaatsuskoolitusele, teadlikkusele ja pädevusele privaatsusteabe haldussüsteemis.

1.2 Käesolevat poliitikat kohaldatakse personalile, töövõtjatele, ajutisele personalile, asjakohastele kolmandatele osapooltele, volitatud töötlejatele, alltöötlejatele ja muudele huvitatud osapooltele, kelle töö võib mõjutada PII töötlemist, PIMS-i toimivust, isikuandmesubjekti õigusi, privaatsusriski, PII-ga seotud infoturvet, volitatud töötleja juhiseid, privaatsusintsidente, dokumenteeritud teavet või vastavustõendeid.

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

1.4 Käesolev poliitika hõlmab järgmist:

1.4.1 privaatsuskoolituse sihtrühmade tuvastamine;

1.4.2 sisseelamiskoolitus;

1.4.3 iga-aastane korduskoolitus;

1.4.4 rollipõhine ja sündmusepõhine koolitus;

1.4.5 koolituse läbimise tõendusmaterjal;

1.4.6 läbimata koolituse eskaleerimine;

1.4.7 koolituse tõhususe läbivaatamine;

1.4.8 volitatud töötleja, alltöötleja ja kolmanda osapoole koolituse kindlust andev tõendusmaterjal.

1.5 Käesolev poliitika ei loo eraldi koolitusmaatriksit, koolituse juhtpaneeli, personaliregistrit, pädevusregistrit, distsiplinaarregistrit ega kliendikoolituse registrit. Koolituste määramised, läbimised, meeldetuletused, pädevustõendid ja teadlikkuse tõendusmaterjal registreeritakse REG11-s ning erandid, eskaleerimised, mittevastavused, parandusmeetmed ja läbivaatamise tõendusmaterjal registreeritakse REG12-s. Volitatud töötleja, alltöötleja ja kolmanda osapoole koolituse kindlust andev tõendusmaterjal registreeritakse asjakohasel juhul REG08-s.

1.6 Käesolev poliitika ei dubleeri järgmist:

1.6.1 rollivastutuse määramine PII02-s;

1.6.2 töötlemisregister ja õigusliku aluse nõuded PII03-s;

1.6.3 privaatsusriski ja DPIA metoodika PII07-s;

1.6.4 lõimitud andmekaitse põhimõtte kontrolliväravad PII08-s;

1.6.5 volitatud töötleja elutsükli juhtimine PII12-s;

1.6.6 PII turvalisuse ja juurdepääsukontrolli toimimine PII14-s;

1.6.7 PII intsidendi ja rikkumise töövoog PII15-s;

1.6.8 dokumenteeritud teabe juhtimine PII17-s;

1.6.9 seire, siseauditi ja täiustamise juhtimine PII18-s.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et isikud, kelle töö mõjutab PII töötlemist, mõistavad oma privaatsusega seotud vastutusi, läbivad asjakohase koolituse määratud sagedusega, säilitavad rolliga seotud pädevuse ning loovad koolituse, teadlikkuse ja eskaleerimise kohta auditiks sobiva tõendusmaterjali.

2.2 Käesolev poliitika toetab PIMS-i järjepidevat rakendamist, kasutades REG11-t koolituse ja teadlikkuse esmase tõendusobjektina ning REG08-t, REG10-t ja REG12-t toetavate tõendusobjektidena.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 määratleda privaatsuskoolituse sihtrühmad;

3.1.2 määratleda sisseelamiskoolituse nõuded;

3.1.3 määratleda iga-aastase korduskoolituse nõuded;

3.1.4 määratleda rollipõhise privaatsuskoolituse nõuded;

3.1.5 registreerida läbimise tõendusmaterjal REG11-s;

3.1.6 eskaleerida läbimata koolitused REG12 kaudu;

3.1.7 säilitada asjakohasel juhul REG08-s volitatud töötlejate, alltöötlejate ja kolmandate osapoolte koolituse kindlust andev tõendusmaterjal;

3.1.8 vaadata läbi koolituse tõhusus ilma liigseid mõõdikuid või dubleerivaid registreid loomata;

3.1.9 tagada, et koolituse sisu püsib kooskõlas kehtivate PIMS-i poliitikate ja oluliste privaatsuskohustustega.

4. Poliitikapõhimõtted

4.1 Koolituse sihtrühm ja määramine

4.1.1 [All] Privacy Lead / PIMS Manager peab enne iga iga-aastase koolitustsükli algust määratlema PIMS-i koolituse sihtrühmade kategooriad REG11-s.

4.1.2 [All] Process Owner / Business Owner peab enne tööle asumist, rolli määramist või olulist tööülesannete muudatust tuvastama REG11-s personali, kelle tööülesanded hõlmavad PII töötlemist.

4.1.3 [Conditional] System Owner / Application Owner peab enne juurdepääsu lubamist või olulist muutmist tuvastama REG11-s kasutajad, kes vajavad PII süsteemi, privilegeeritud juurdepääsu või haldusõigustega seotud privaatsuskoolitust.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager peab enne ühise töötlemistoimingu algust või olulist muutmist registreerima kaasvastutavate töötlejate koolitusvastutuse jaotuse REG11-s või REG08-s.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor peab enne koolituse määramist rollidele, mis käsitlevad kõrge riskiga töötlemist, eriliiki PII-d, isikuandmesubjekti õigusi, DPIAs, rahvusvahelisi edastusi või rikkumise hindamist, tuvastama REG11-s tõhustatud privaatsuskoolituse vajadused.

4.1.6 [All] Privacy Lead / PIMS Manager peab enne iga iga-aastase koolitustsükli algust registreerima REG11-s määratud koolituse sihtrühma, koolituse liigi, nõutava läbimise kuupäeva ja tõendusmaterjali omaniku.

4.2 Sisseelamise ja iga-aastase koolituse sagedus

4.2.1 [All] Privacy Lead / PIMS Manager peab määrama REG11-s privaatsusteadlikkuse baaskoolituse 10 tööpäeva jooksul pärast tööle asumist personalile, kellel on juurdepääs PII-le või PIMS-i vastutused.

4.2.2 [All] Process Owner / Business Owner peab tagama, et määratud personal läbiks sisseelamiskoolituse privaatsuse alal REG11-s enne järelevalveta juurdepääsu heakskiitmist PII-le või 30 päeva jooksul pärast tööle asumist, olenevalt sellest, kumb toimub varem.

4.2.3 [All] Privacy Lead / PIMS Manager peab määrama REG11-s iga-aastase privaatsuse korduskoolituse vähemalt kord iga 12 kuu jooksul.

4.2.4 [All] Process Owner / Business Owner peab kinnitama määratud personali iga-aastase korduskoolituse läbimise staatuse REG11-s avaldatud iga-aastaseks tähtajaks.

4.2.5 [Conditional] Privacy Lead / PIMS Manager peab määrama REG11-s sihitud korduskoolituse 30 päeva jooksul pärast olulist privaatsuspoliitika muudatust, olulist PIMS-i

protsessimuudatust, auditileidu, korduvat koolituse läbikukkumist või asjakohast PII intsidendi õppetundi.

[... 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 nõutava läbimise tähtaja pikendamist registreerima REG12-s privaatsuskoolituse eranditaotluse.

9.1.2 [All] Privacy Lead / PIMS Manager peab enne erandi aktiveerumist REG12-s privaatsuskoolituse eranditaotlused heaks kiitma või tagasi lükkama.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor peab enne heakskiitmist nõustama REG12-s koolituserandite osas, kui erand mõjutab kõrge riskiga töötlemist, eriliiki PII-d, õiguste käsitlemist, intsidentide käsitlemist, rahvusvahelisi edastusi või sertifitseerimistõendeid.

9.1.4 [Conditional] Top Management peab enne aktiveerimist heaks kiitma REG12-s privaatsuskoolituse erandid, kui erand mõjutab korduvat läbimata jätmist, privilegeeritud PII juurdepääsu, suure mõjuga PII töötlemist või regulatiivse suunitlusega tõendusmaterjali.

9.1.5 [All] Privacy Lead / PIMS Manager peab enne mis tahes privaatsuskoolituse erandi heakskiitmist määratlema REG12-s erandi omaniku, aegumiskuupäeva, kompenseeriva tegevuse ja läbivaatamise kuupäeva.

9.1.6 [All] Process Owner / Business Owner peab enne erandi aegumiskuupäeva sulgema või uuendama REG12-s heakskiidetud privaatsuskoolituse erandid.

10. Järgimise tagamine

10.1.1 [All] Privacy Lead / PIMS Manager peab viie tööpäeva jooksul registreerima REG12-s koolituse mittevastavuse, kui kohustusliku privaatsuskoolituse tõendusmaterjal puudub, on mittetäielik, tähtaja ületanud või ei ole REG11-ni jälgitav.

10.1.2 [All] Process Owner / Business Owner peab tagama, et tähtaja ületanud kohustuslik privaatsuskoolitus läbitakse või eskaleeritakse REG11-s või REG12-s 10 tööpäeva jooksul pärast tähtaja ületamise staatuse registreerimist.

10.1.3 [Conditional] System Owner / Application Owner peab piirama REG12-s uut suure mõjuga PII juurdepääsu, kui nõutav sisseelamis- või rollipõhine privaatsuskoolitus on pärast eskaleerimist endiselt läbimata.

10.1.4 [Processor] Vendor / Procurement Owner peab viie tööpäeva jooksul pärast tuvastamist eskaleerima REG08-s ja REG12-s puuduva volitatud töötleja, alltöötleja või välise tööjõu koolituse kindlust andva tõendusmaterjali.

10.1.5 [Conditional] Incident Response Coordinator peab ühe tööpäeva jooksul siduma koolitusega seotud rakendamismeetmed REG10-ga, kui koolituse puudus aitas kaasa kahtlustatavale või kinnitatud PII intsidendile.

10.1.6 [All] Internal Audit / Compliance Reviewer peab kontrollima REG12-s koolituse parandusmeetmete sulgemise tõendusmaterjali järgmisel plaanitud 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 vähemalt kord aastas läbi vaatama käesoleva poliitika ja koolituse sisu ning registreerima läbivaatamise tulemuse REG11-s või REG12-s.

11.1.2 [All] Privacy Lead / PIMS Manager peab käesoleva poliitika läbi vaatama 30 päeva jooksul pärast olulist muudatust PIMS-i kohaldamisalas, privaatsusõiguses, töötlemistoimingutes, rollimudelis, intsidendi õppetundides, auditileidudes või koolituse tõhususe tulemustes.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor peab enne heakskiitmist läbi vaatama REG12-s privaatsuse seisukohast olulised poliitikamuudatused.

11.1.4 [All] Top Management peab enne avaldamist heaks kiitma REG12-s käesoleva poliitika olulised muudatused.

11.1.5 [All] Privacy Lead / PIMS Manager peab 30 päeva jooksul pärast heakskiidetud olulist poliitikamuudatust ajakohastama REG11-s koolituse sisu ja määramise tõendusmaterjali.

12. Seotud poliitikad

12.1 Käesolevat poliitikat tuleb lugeda koos järgmiste dokumentidega:

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 - Privaatsusriski hindamise ja DPIA poliitika;

12.9 PII08 - Lõimitud ja vaikimisi andmekaitse poliitika;

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

12.11 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika;

12.12 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsushalduse poliitika;

12.13 PII13 - Rahvusvahelise PII edastamise poliitika;

12.14 PII14 - PII turvalisuse ja juurdepääsukontrolli poliitika;

12.15 PII15 - PII intsidendi ja rikkumise haldamise poliitika;

12.16 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali haldamise poliitika;

12.17 PII18 - PIMS-i seire, auditi ja täiustamise poliitika.

13. Viitestandardid ja raamistikud

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].