					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: PII02					Dokumendi pealkiri: **Privaatsusrollide, vastutuste ja vastutuse 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 / regulatsioon	Punkt / kontrollimeede / artikkel	Kohaldatavus	Katvuse tüüp	Kommentaar
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	PIMS-i rolli kontekst
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Juhtimine ja vastutus
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS-i rollid, vastutused ja volitused
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Rollipädevus
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Rolliteadlikkus
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Rollidega seotud teabevahetus
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Rollidega seotud dokumenteeritud teave
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operatiivse kontrolli omamine
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Sõltumatu auditi roll
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vastutuse juhtkonnapoolne läbivaatamine
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Rolliga seotud mittevastavus ja parandusmeede
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Volitatud töötleja lepingu vastutus
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Kaasvastutavate töötlejate rollid ja vastutused
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Vastutuse kirjed
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Volitatud töötleja kliendikokkulepped ja juhised
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Volitatud töötleja eesmärkide kooskõla

GDPR	Article 5(2)	Controller	Supporting	Vastutuse tõendusmaterjal
GDPR	Article 24	Controller	Supporting	Vastutava töötleja vastutus ja meetmed
GDPR	Article 26	Joint Controller	Supporting	Kaasvastutavate töötlejate kokkulepped
GDPR	Article 28	Both	Supporting	Volitatud töötleja juhtimine ja juhised
GDPR	Article 30	Both	Supporting	Töötlemise kirjed ja vastutuse tõendusmaterjal
GDPR	Article 37	Conditional	Referenced	Andmekaitseametniku määramine, kui kohaldatav
GDPR	Article 38	Conditional	Supporting	Andmekaitseametniku positsioon ja sõltumatus, kui kohaldatav
GDPR	Article 39	Conditional	Supporting	Andmekaitseametniku ülesanded, kui kohaldatav
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Privaatsusraamistiku osalised ja rollid
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privaatsusnõuete täitmise vastutus
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	PII kaitse rollid ja lahusus
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Infoturbe rollid ja vastutused
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Ülesannete lahusus

1. Kohaldamisala

1.1 Käesolev poliitika määratleb PIMS-i rollimudeli, vastutuse struktuuri, vastutuste määramise reeglid, rollide kombineerimise reeglid, eskaleerimise ootused ja tõendusmaterjali nõuded privaatsuse juhtimiseks.

1.2 Käesolev poliitika kohaldub personalile, funktsioonidele, süsteemidele, tarnijatele, volitatud töötlejatele, alltöötlejatele ja kaasvastutavate töötlejate suhetele, mis osalevad PII töötlemises või mõjutavad seda PIMS-i kohaldamisala piires.

1.3 Käesolev poliitika kohaldub vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kontekstides.

1.4 Käesolev poliitika ei loo uusi organisatsioonilisi ametinimetusi. See määratleb kanoonilised PIMS-i rollid, mida võib määrata olemasolevale personalile või funktsioonidele, eeldusel et rolli määramine, pädevus, sõltumatus ja huvide konflikti nõuded on dokumenteeritud.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et PIMS-i vastutused on selgelt määratud, mõistetud, edastatud, tõendatud, läbi vaadatud ja täiustatud.

2.2 Käesolev poliitika võimaldab organisatsioonil tõendada vastutust privaatsuse juhtimise, PII töötlemise omamise, vastutava ja volitatud töötleja rolli määramise, kaasvastutavate töötlejate vastutuste jaotamise, volitatud töötleja juhiste käsitlemise, tarnija privaatsusvastutuse, sõltumatu läbivaatamise ning rollipõhise eskaleerimise eest.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 määratleda PIMS-i poliitikakomplektis kasutatavad kanoonilised PIMS-i rollid;

3.1.2 tagada, et igal olulisel PIMS-i vastutusel on määratud vastutav roll;

3.1.3 toetada vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja vastutust;

3.1.4 võimaldada väikestes ja keskmise suurusega organisatsioonides rollide praktilist kombineerimist, kontrollides samal ajal huvide konflikte;

3.1.5 säilitada sõltumatu läbivaatamine Internal Audit / Compliance Reviewer rolli kaudu;

3.1.6 tagada, et rollimäärangud ja rollimuudatused registreeritakse kanoonilistes tõendusobjektides;

3.1.7 tagada, et PIMS-i rollide kandjad saavad asjakohast teabevahetust ja teadlikkust;

3.1.8 tagada, et rollidega seotud puudujäägid, konfliktid ja mittevastavused eskaleeritakse ja parandatakse.

4. Poliitika põhimõtted

4.1 PIMS-i rollimudel ja määramine

4.1.1 [All] Top Management PEAB kinnitama kanoonilise PIMS-i rollimudeli registris REG01 enne PIMS-i esmast rakendamist ja seejärel igal aastal.

4.1.2 [All] Privacy Lead / PIMS Manager PEAB hoidma nimelisi PIMS-i rollimääranguid registris REG01 enne PIMS-i rakendamist ning 10 tööpäeva jooksul pärast personali- või organisatsioonilisi muudatusi.

4.1.3 [All] Privacy Lead / PIMS Manager PEAB dokumenteerima iga määratud PIMS-i rolli vastutusala ja volituste taseme registris REG01 enne määrangu jõustumist.

4.1.4 [All] Process Owner / Business Owner PEAB määrama iga PII töötlemistoimingu jaoks vastutava töötlemise omaniku registris REG02 enne töötlemistoimingu alustamist.

4.1.5 [All] System Owner / Application Owner PEAB dokumenteerima iga PII-d töötleva süsteemi vastutava süsteemiomaniku registris REG02 enne süsteemi tootmiskeskkonda kasutuselevõttu.

4.1.6 [All] Vendor / Procurement Owner PEAB dokumenteerima iga volitatud töötleja, alltöötleja, kolmandale osapoolele andmete jagamise või kaasvastutava töötleja suhte omaniku registris REG08 enne kaasamist või kokkuleppe kinnitamist.

4.2 Rollide kombineerimine, lahusus ja sõltumatus

4.2.1 [All] Privacy Lead / PIMS Manager PEAB dokumenteerima iga PIMS-i rollide kombineerimise registris REG01 enne rollide kombineerimise jõustumist.

4.2.2 [All] Top Management PEAB kinnitama rollide kombineerimised, mis hõlmavad rolle Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator või Internal Audit / Compliance Reviewer, registris REG01 enne määramist.

4.2.3 [All] Internal Audit / Compliance Reviewer PEAB dokumenteerima sõltumatuse läbivaadatavast PIMS-i protsessist registris REG12 enne iga PIMS-i auditi või vastavuse ülevaatuse alustamist.

4.2.4 [All] Privacy Lead / PIMS Manager PEAB registreerima vältimatute lahususe konfliktide kompenseerivad kontrollimeetmed registris REG12 enne rollide kombineerimise kinnitamist.

4.2.5 [All] Data Protection Officer / Privacy Advisor PEAB registreerima rolli sõltumatusega seotud probleemid või huvide konflikti probleemid registris REG12 viie tööpäeva jooksul pärast tuvastamist.

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

9. Erandid

9.1.1 [All] Process Owner / Business Owner PEAB taotlema rollivastutuse erandit registris REG12 enne PII töötlemistoimingu käitamist ilma nõutava määratud rollita.

9.1.2 [All] Privacy Lead / PIMS Manager PEAB hindama iga rollivastutuse erandi mõju ja leevendamist registris REG12 10 tööpäeva jooksul pärast taotlust.

9.1.3 [All] Top Management PEAB kinnitama rollivastutuse erandid, mis ületavad 30 päeva või mõjutavad kõrge riskiga töötlemist, registris REG12 enne erandi jõustumist.

9.1.4 [All] Privacy Lead / PIMS Manager PEAB määrama iga kinnitatud rollivastutuse erandi jaoks registris REG12 enne kinnitamist aegumiskuupäeva, mis ei ületa 90 päeva.

9.1.5 [All] Privacy Lead / PIMS Manager PEAB sulgema või uuesti hindama iga rollivastutuse erandi registris REG12 viie tööpäeva jooksul pärast aegumist.

10. Järgimise tagamine

10.1.1 [All] Privacy Lead / PIMS Manager PEAB registreerima puuduvad, ebatäpsed või aegunud PIMS-i rollimäärangud mittevastavustena registris REG12 viie tööpäeva jooksul pärast tuvastamist.

10.1.2 [All] Top Management PEAB nõudma parandusmeetmeid registris REG12 15 tööpäeva jooksul korduvate või pikaajaliste vastutuse puuduste korral.

10.1.3 [All] Process Owner / Business Owner PEAB takistama uue või muudetud PII töötlemise tootmiskeskkonda kasutuselevõttu, kui nõutav rolli- ja vastutuse tõendusmaterjal puudub registrist REG02 või REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer PEAB kontrollima rollivastutuse mittevastavuste parandusmeetmete tõhusust registris REG12 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 vaatama käesoleva poliitika läbi kord aastas ja 30 päeva jooksul pärast PIMS-i rollimudeli olulist muudatust.

11.1.2 [All] Data Protection Officer / Privacy Advisor PEAB vaatama käesoleva poliitika kavandatud muudatused privaatsusrollide mõju seisukohast läbi registris REG12 enne kinnitamist.

11.1.3 [All] Top Management PEAB kinnitama käesoleva poliitika olulised muudatused registris REG12 enne avaldamist.

11.1.4 [All] Privacy Lead / PIMS Manager PEAB ajakohastama REG01 ja REG11 15 tööpäeva jooksul pärast PIMS-i rollide, vastutuste või teabevahetuse nõuete kinnitatud muudatusi.

12. Seotud poliitikad

12.1 Käesolevat poliitikat toetavad järgmised seotud poliitikad:

12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika

12.3 PII03 - PII töötlemise inventuuri ja õigusliku aluse poliitika

12.4 PII07 - Privaatsusriskide hindamise ja DPIA poliitika

12.5 PII08 - Lõimitud ja vaikimisi privaatsuse poliitika

12.6 PII12 - Volitatud töötlejate, alltöötlejate ja kolmandate osapoolte privaatsuse halduse poliitika

12.7 PII14 - PII turbe ja juurdepääsukontrolli poliitika

12.8 PII15 - PII intsidentide ja rikkumiste halduse poliitika

12.9 PII16 - Privaatsuskoolituse, teadlikkuse ja pädevuse poliitika

12.10 PII17 - PIMS-i dokumenteeritud teabe ja tõendusmaterjali halduse poliitika

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

13. Viitestandardid ja raamistikud

13.1 Käesolev poliitika on vastendatud järgmiste standardite ja regulatsioonidega. Vastendus selgitab, kuidas poliitika toetab viidatud nõudeid, ning tuvastab sisemised punktid, millega neid rakendatakse või toetatakse.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Vastendatud PIMS-i rollikonteksti määramise, vastutava ja volitatud töötleja kohaldatavuse, töötlemise omamise ning suhete vastutuse kirjete haldamisega. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Vastendatud Top Management heakskiidu, vastutuse järelevalve, iga-aastase juhtkonna läbivaatamise, vastutuse mõõdikute ja rollipuuduste parandusmeetmetega. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Vastendatud PIMS-i rollide, vastutuste, volituste, süsteemi omamise, töötlemise omamise, tarnijasuhte omamise, intsidendi eskaleerimise omamise ja sõltumatu läbivaatamise vastutuse määramise, dokumenteerimise, teavitamise ja hoidmisega. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Vastendatud määratud PIMS-i vastutuste rollipõhise pädevuse ja teadlikkuse tõendusmaterjaliga. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Vastendatud määratud PIMS-i vastutuste teadlikkuse, kinnituse tõendusmaterjali ja iga-aastase rolliteadlikkuse aruandlusega. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Vastendatud rollimäärangute, rollimuudatuste, eskaleerimiste ja rolli üleandmise teabe edastamisega. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Vastendatud dokumenteeritud teabega PIMS-i rollimäärangute, vastutusalade, volituste tasemete, iga-aastase tõendusmaterjali säilitamise ja rollimaatriksi hoidmise kohta. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Vastendatud töötlemistoimingute, süsteemide, tarnijate, volitatud töötlejate, alltöötlejate, kaasvastutavate töötlejate suhete ja tootmiskeskkonda kasutuselevõtu kontrollide operatiivse kontrolli omamisega. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Vastendatud rollimäärangute tõendusmaterjali, rollide kombineerimise tõendusmaterjali, sõltumatuse tõendusmaterjali, leidude ja parandusmeetmete sulgemise sõltumatu auditi ja vastavuse ülevaatusega. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Vastendatud PIMS-i rollimäärangute täielikkuse, rollikonfliktide, erandite, vastutuse mõõdikute ja vastutuse läbivaatamise väljundite juhtkonnapoolse läbivaatamisega. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Vastendatud rollivastutuse probleemide eskaleerimise, mittevastavuste registreerimise, parandusmeetmete, erandite sulgemise ja tõhususe kontrollimisega. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Vastendatud volitatud töötleja lepingu vastutuse määramise ja dokumenteerimisega ning kolmanda osapoole vastutuse eskaleerimisega enne lepingu kinnitamist või uuendamist. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Vastendatud kaasvastutavate töötlejate vastutusvaldkondade jaotuse ja suhte vastutuse tõendusmaterjali dokumenteerimisega enne kaasvastutavate töötlejate töötlemise alustamist. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Vastendatud vastutava töötleja töötlemise omamise, rolliklassifikatsiooni ja tõendusmaterjali omamise vastutuse kirjete hoidmisega. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Vastendatud volitatud töötleja kliendikokkuleppe vastutuse, kliendijuhiste omamise ja volitatud töötleja suhte tõendusmaterjaliga. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Vastendatud volitatud töötleja eesmärgi ja juhiste kooskõlaga kliendijuhiste omamise ning vastutava ja volitatud töötleja rolli kontrollimise kaudu. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Vastendatud rollimäärangute, töötlemise omamise, rollide läbivaatamiste, mittevastavuste ja auditileidude vastutuse tõendusmaterjaliga. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Vastendatud vastutava töötleja vastutuse, vastutava töötlemise omamise, Top Management järelevalve, iga-aastase läbivaatamise ja vastutusmeetmetega. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Vastendatud kaasvastutavate töötlejate vastutusvaldkondade jaotuse ja suhte vastutuse tõendusmaterjali dokumenteerimisega enne kaasvastutavate töötlejate töötlemise alustamist. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Vastendatud volitatud töötleja ja alltöötleja vastutusvaldkondade jaotuse, kliendijuhiste omamise, lepingu vastutuse ja kolmanda osapoole eskaleerimisteedega. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Vastendatud töötlemise kirjete, töötlemise omamise, PIMS-i rolliklassifikatsiooni ning vastutava ja volitatud töötleja rolli kontrollimisega. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Vastendatud Data Protection Officer / Privacy Advisor rolli dokumenteerimisega, kui määramine on kohaldatav või roll on vabatahtlikult määratud. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Vastendatud Data Protection Officer / Privacy Advisor rolli positsiooni, sõltumatuse, kaasamise ja huvide konflikti käsitlemisega, kui see on kohaldatav. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Vastendatud Data Protection Officer / Privacy Advisor rolli privaatsusnõu, seire tähelepanekute, nõustava läbivaatamise ja rolliga seotud privaatsusmõju läbivaatamisega, kui see on kohaldatav. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Vastendatud privaatsusraamistiku osaliste ja rollide jaotamisega isikuandmesubjektide, PII vastutavate töötlejate, PII volitatud töötlejate, kolmandate osapoolte ja PIMS-i rolliklassifikatsiooni jaoks. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Vastendatud privaatsusnõuete täitmise vastutuse, rollide tõendusmaterjali, läbivaatamise, auditileidude ja parandusmeetmete tõhususe kontrollimisega. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Vastendatud PII kaitse rollide määratlemise, rollide dokumenteerimise, rollidega seotud teabevahetuse, turbe ja privaatsuse koordineerimise ning PII kaitse ülesannete lahususega. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Vastendatud PIMS-i ja infoturbe vastutuste määratlemise, jaotamise, dokumenteerimise, teavitamise ja hoidmisega. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Vastendatud ülesannete lahususe, rollide kombineerimise kinnitamise, sõltumatu läbivaatamise, konfliktikontrollide ja rollikonfliktide parandusmeetmete tõhususe kontrollimisega. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].