					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: PII14					Dokumendi pealkiri: **PII turbe ja juurdepääsukontrolli 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 liik	Kommentaar
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	PII turbekontrollide kavandamine ja toimimine
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Tõendusmaterjal, seire ja parandusmeetmed
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identiteet ja juurdepääsuõigused PII töötlemiseks
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Lõppseadmete kaitse ja turvaline autentimine
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logimine ja krüptograafiline kaitse
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Rakendusturve ja turvaline arhitektuur
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Kirjete kaitse ja läbivaatamine
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Turvalisus, vastutus ja volitatud töötleja kontrollimeetmed
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	ISMS kontrollimeetmete integreerimine
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Turbekontrollide rakendamise juhised
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Infoturbe ja privaatsuse vastavuspõhimõtted
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2;	Both	Supporting	PII kaitse turbekontrollid

	Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Kohaldamisala

1.1 Käesolev poliitika määrab PII-spetsiifilised turbe- ja juurdepääsukontrolli nõuded süsteemidele, rakendustele, teenustele, seadmetele, pilvekeskkondadele ja operatiivprotsessidele, mis säilitavad, edastavad, töötlevad, kasutavad, haldavad või kaitsevad PII.

1.2 Käesolev poliitika kohaldub vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kontekstides, kus organisatsioon määrab, käitab, toetab või kasutab PII töötlemise turbekontrolle.

1.3 Käesolev poliitika hõlmab järgmisi PII turbekontrolli valdkondi:

1.3.1 PII turbe baastase ja integreerimine olemasolevate infoturbepoliitikatega;

1.3.2 juurdepääsukontroll;

1.3.3 autentimine;

1.3.4 privilegeeritud juurdepääs;

1.3.5 krüptimine ja turvaline salvestamine;

1.3.6 logimine ja seire;

1.3.7 turvaline seadistamine ja haavatavuste haldus;

1.3.8 lõppseadmete ja pilve juurdepääsukontrollid;

1.3.9 tõendusmaterjali seostamine objektidega REG02, REG08, REG10 ja REG12.

1.4 Käesolev poliitika ei asenda terviklikku infoturbe juhtimissüsteemi, võrguturbe poliitikat, turvalise arenduse poliitikat, varunduspoliitikat, lõppseadmete poliitikat, pilveturbe poliitikat, krüptograafilist standardit, haavatavuste halduse protseduuri ega intsidentidele reageerimise protseduuri. Kui sellised poliitikad on juba olemas, määrab käesolev poliitika PII-spetsiifilised seosed ja tõendusmaterjali nõuded, mida on vaja PIMS kindluse andmiseks.

1.5 Käesolev poliitika ei dubleeri:

1.5.1 PII töötlemise registrit ja õigusliku aluse vastutust poliitikas PII03;

1.5.2 privaatsusriskide ja DPIA metoodikat poliitikas PII07;

1.5.3 privaatsus kavandamisel kontrollpunkte poliitikas PII08;

1.5.4 kogumise, kasutamise, avalikustamise ja jagamise reegleid poliitikas PII09;

1.5.5 säilitamise, kustutamise ja kõrvaldamise teostamist poliitikas PII10;

1.5.6 volitatud töötleja elutsükli juhtimist poliitikas PII12;

1.5.7 rahvusvahelise edastamise mehhanismide kontrollimeetmeid poliitikas PII13;

1.5.8 intsidendi ja rikkumise töövoogu poliitikas PII15;

1.5.9 dokumenteeritud teabe juhtimist poliitikas PII17;

1.5.10 PIMS seire, auditi ja täiustamise juhtimist poliitikas PII18.

1.6 Käesolevas poliitikas on operatiivlogid, turbetööriistade väljundid, juurdepääsuõiguste läbivaatamise ekspordid, haavatavuste aruanded ja konfiguratsiooni tõendusmaterjal tõendusallikad, mis lisatakse kanoonilistele tõendusmaterjali objektidele, võetakse neis kokku või millele neis viidatakse. Need ei ole eraldi PIMS registrid.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et PII oleks kogu töötlemise vältel kaitstud asjakohaste, riskiga kooskõlas olevate ja auditeeritavate turbe- ja juurdepääsukontrollidega.

2.2 Käesolev poliitika võimaldab organisatsioonil tõendada, et PII turbekontrollid on kavandatud, rakendatud, läbi vaadatud, seiratud ja täiustatud objektide REG02, REG08, REG10 ja REG12 kaudu, loomata dubleerivaid turberegistreid ega asendamata olemasolevaid infoturbepoliitikaid.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 määrata PII juurdepääsukontrolli baastase süsteemidele ja töötlemistoimingutele;

3.1.2 tagada, et autentimiskontrollid vastaksid PII tundlikkusele ja juurdepääsu kontekstile;

3.1.3 määrata PII-le privilegeeritud ja tavapärase juurdepääsu läbivaatamise nõuded;

3.1.4 määrata PII krüptimise ja turvalise salvestamise ootused puhkeolekus, edastamisel ning asjakohastes pilve- või lõppseadme kontekstides;

3.1.5 määrata logimise ja seire ootused seoses juurdepääsuga PII, PII muudatustega ja PII haldamisega;

3.1.6 määrata turvalise seadistamise ja haavatavuste tõendusmaterjali nõuded süsteemidele, mis töötlevad PII;

3.1.7 määrata lõppseadmete ja pilve juurdepääsu ootused, loomata terviklikku lõppseadmete või pilveturbe poliitikat;

3.1.8 seostada kahtlustatavad PII turbeintsidendid objektiga REG10, dubleerimata intsidendi töövoogu;

3.1.9 integreerida olemasolevate infoturbepoliitikatega, kui need on olemas;

3.1.10 säilitada auditiks valmis tõendusmaterjal ainult objektide REG02, REG08, REG10 ja REG12 abil.

4. Poliitika põhimõtted

4.1 PII turbe baastase ja ISMS integreerimine

4.1.1 [Both] Information Security Lead MUST määrama iga PII töötleva süsteemi või teenuse PII turbe baastaseme objektis REG12 enne süsteemi või teenuse tootmiskeskkonda viimist või olulist muutmist.

4.1.2 [Both] System Owner / Application Owner MUST registreerima rakendatud PII turbekontrolli tõendusmaterjali asukoha objektis REG12 enne olemasolevale infoturbe kontrollimeetmele tuginemist PIMS kindluse andmiseks.

4.1.3 [Controller] Process Owner / Business Owner MUST tuvastama PII tundlikkuse, töötlemise konteksti ja juurdepääsuvajaduse objektis REG02 enne uue või oluliselt muudetud juurdepääsu taotlemist PII.

4.1.4 [Processor] Vendor / Procurement Owner MUST registreerima kliendi turbejuhised, kliendi vastutuse piirid ja volitatud töötleja turbega seotud kohustused objektis REG08 enne, kui algab või oluliselt muutub volitatud töötleja juurdepääs kliendi PII.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST kontrollima, et PII turbe tõendusmaterjal oleks seotud objektiga REG02, REG08, REG10 või REG12 enne töötlemistoimingu aktsepteerimist PIMS jaoks auditiks sobivana.

4.2 Juurdepääsukontrolli baastase

4.2.1 [Both] System Owner / Application Owner MUST piirama juurdepääsu PII heakskiidetud rollide ja volitatud kasutajatega, kes on registreeritud või jälgitavad objektis REG02 või REG12, enne juurdepääsu lubamist.

4.2.2 [Both] Process Owner / Business Owner MUST heaks kiitma PII juurdepääsu ärilise eesmärgi objektis REG02 või REG12 enne, kui System Owner / Application Owner annab juurdepääsuõigused.

4.2.3 [Both] System Owner / Application Owner MUST vaatama vähemalt kord kvartalis läbi kasutajate juurdepääsu süsteemidele, mis töötlevad suure mõjuga PII või tundlikku PII, ning registreerima läbivaatamise tulemuse objektis REG12.

4.2.4 [Both] System Owner / Application Owner MUST vaatama vähemalt kord aastas läbi kasutajate juurdepääsu muudele süsteemidele, mis töötlevad PII, ning registreerima läbivaatamise tulemuse objektis REG12.

4.2.5 [Both] System Owner / Application Owner MUST eemaldama või muutma PII juurdepääsu objektis REG12 ühe tööpäeva jooksul pärast rollimuudatust, töösuhte lõpetamist, lepingu lõppemist või juurdepääsuvajaduse lõppemist.

4.2.6 [Processor] Vendor / Procurement Owner MUST kinnitama objektis REG08, et volitatud töötleja juurdepääs kliendi PII on piiratud dokumenteeritud kliendi juhistega, enne juurdepääsu lubamist või muutmist.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST kinnitama objektis REG08, et alltöötleja juurdepääs PII on piiratud lubatud alltöötlustoimingutega, enne alltöötleja juurdepääsu lubamist või muutmist.

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

9. Erandid

9.1.1 [Both] Information Security Lead MUST registreerima iga erandi PII turbe- või juurdepääsukontrolli nõudest objektis REG12 enne erandi aktiveerimist.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST andma nõu kõrgema riskiga PII turbeerandite kohta objektis REG12 enne heakskiitu.

9.1.3 [Both] Top Management MUST heaks kiitma PII turbeerandid objektis REG12 enne aktiveerimist, kui erand mõjutab suure mõjuga PII, tundlikku PII, privilegeeritud juurdepääsu, krüptimist, logimist või lahendamata kõrge riskiga haavatavusi.

9.1.4 [Both] Information Security Lead MUST määrama erandi aegumise, kompenseeriva kontrollimeetme ja läbivaatamise kuupäeva objektis REG12 enne erandi heakskiitu.

9.1.5 [Both] System Owner / Application Owner MUST parandama, uuendama või sulgema aegunud PII turbeerandid objektis REG12 viie tööpäeva jooksul pärast aegumist.

9.1.6 [Processor] Vendor / Procurement Owner MUST registreerima kliendi PII mõjutavad volitatud töötleja või alltöötleja turbeerandid objektides REG08 ja REG12 enne aktsepteerimist.

10. Järgimise tagamine

10.1.1 [Both] Privacy Lead / PIMS Manager MUST registreerima mittevastavused puuduva või mittetäieliku PII turbe tõendusmaterjali kohta objektis REG12 viie tööpäeva jooksul pärast tuvastamist.

10.1.2 [Both] Information Security Lead MUST määrama PII turbekontrolli tõrgete parandamise vastutuse objektis REG12 viie tööpäeva jooksul pärast valideerimist.

10.1.3 [Both] System Owner / Application Owner MUST keelama või piirama volitamata, ülemäärase või tõendusmaterjaliga toetamata PII juurdepääsu ühe tööpäeva jooksul pärast valideerimist ning registreerima toimingu objektis REG12.

10.1.4 [Conditional] Incident Response Coordinator MUST seostama järgimise tagamise toimingud objektiga REG10 ühe tööpäeva jooksul, kui järgimise tagamise küsimus hõlmab kahtlustatavat või kinnitatud PII intsidenti.

10.1.5 [Both] Top Management MUST vaatama korduvad või kõrge riskiga PII turbe mittevastavused läbi objektis REG12 enne juhtkonna läbivaatamist.

11. Läbivaatamine ja ajakohastamine

11.1.1 [All] Privacy Lead / PIMS Manager MUST vaatama käesoleva poliitika koos rolliga Information Security Lead läbi vähemalt kord aastas ning registreerima läbivaatamise tulemuse objektis REG12.

11.1.2 [Both] Information Security Lead MUST vaatama PII turbe baastaseme objektis REG12 läbi 30 päeva jooksul pärast olulist tehnoloogia-, ohu-, auditi-, intsidendi- või regulatiivset muudatust, mis mõjutab PII turvet.

11.1.3 [Both] System Owner / Application Owner MUST uuendama süsteemitaseme PII turbe tõendusmaterjali objektis REG12 30 päeva jooksul pärast olulist arhitektuuri-, juurdepääsu-, konfiguratsiooni-, haavatavuse või logimise muudatust.

11.1.4 [Processor] Vendor / Procurement Owner MUST vaatama volitatud töötleja ja alltöötleja PII turbe vastutuse tõendusmaterjali objektis REG08 läbi 30 päeva jooksul pärast olulist teenuse-, kliendi juhise või alltöötleja muudatust.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST kontrollima poliitika läbivaatamise tõendusmaterjali ja valitud PII turbekontrolli tõendusmaterjali objektis REG12 vastavalt heakskiidetud auditiplaanile.

12. Seotud poliitikad

12.1 Käesolevat poliitikat tuleb lugeda koos järgmiste poliitikatega:

12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika;

12.3 PII02 - Privaatsuse rollide, kohustuste ja vastutuse poliitika;

12.4 PII03 - PII töötlemise registri ja õigusliku aluse poliitika;

12.5 PII07 - Privaatsusriskide hindamise ja DPIA poliitika;

12.6 PII08 - Privaatsuse kavandamisel ja vaikimisi andmekaitse poliitika;

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

12.8 PII10 - PII säilitamise, kustutamise ja kõrvaldamise poliitika;

12.9 PII12 - Volitatud töötleja, alltöötleja ja kolmanda osapoole privaatsuse halduse poliitika;

12.10 PII13 - Rahvusvahelise PII edastamise poliitika;

12.11 PII15 - PII intsidendi ja rikkumise halduse poliitika;

12.12 PII16 - Privaatsuskoolituse, teadlikkuse ja pädevuse poliitika;

12.13 PII17 - PIMS dokumenteeritud teabe ja tõendusmaterjali halduse poliitika;

12.14 PII18 - PIMS seire, auditi ja täiustamise poliitika.

13. Viitestandardid ja raamistikud

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].