					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: PII18					Dokumendi pealkiri: **PIMS-i seire, auditi ja täiustamise 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 6.2	Both	Supporting	Privaatsuseesmärkide mõõtmine
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Seire, auditi ja täiustamise dokumenteeritud teave
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Tegevuse planeerimise ja ohje seire
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Seire, mõõtmine, analüüs ja hindamine
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Siseaudit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Juhtkonna läbivaatamine
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Pidev täiustamine
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Mittevastavus ja parandusmeede
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Vastutava töötleja töötlemiskirjed, mida kasutatakse auditis
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Volitatud töötleja lepingu ja auditialase koostöö tõendusmaterjal
GDPR	Article 5(2)	Controller	Supporting	Vastutuse tõendusmaterjal
GDPR	Article 24	Controller	Supporting	Vastutava töötleja meetmed ja tõhususe läbivaatamine
GDPR	Article 28	Both	Supporting	Volitatud töötleja auditi ja koostöö juhtimine
GDPR	Article 30	Both	Supporting	Töötlemiskirjed, mida kasutatakse auditis
GDPR	Article 32	Both	Supporting	Turvameetmete testimine ja hindamine
GDPR	Article 39	Conditional	Supporting	DPO seire ja auditialased nõuanded, kui kohaldatav

ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privaatsusnõuetele vastavus, audit ja sõltumatu järelevalve
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	PII kaitse läbivaatamine ja vastavuse kontrollid
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Infoturbe seire ja hindamine
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS-i siseauditi tugi
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS-i juhtkonna läbivaatamise tugi
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS-i pideva täiustamise tugi
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS-i mittevastavuse ja parandusmeetmete tugi
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Infoturbe sõltumatu läbivaatamine
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Poliitikate ja standardite vastavuse läbivaatamine
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Juhtimissüsteemi auditi põhimõtted, programm, läbiviimine ja pädevus

1. Kohaldamisala

1.1 Käesolev poliitika määrab kindlaks organisatsiooni nõuded PIMS-i seirele, mõõtmisele, analüüsile, hindamisele, siseauditile, juhtkonna läbivaatamisele, mittevastavuste käsitlemisele, parandusmeetmetele ja pidevale täiustamisele.

1.2 Käesolev poliitika kohaldub järgmisele:

1.2.1 kõik PIMS-i protsessid, kontrollimeetmed, poliitikad, registrid, tõendusmaterjali objektid, süsteemid, tarnijad, volitatud töötlejad, alltöötlejad ja andmete jagamise kokkulepped PIMS-i kohaldamisalas;

1.2.2 organisatsiooni vastutava töötleja, kaasvastutava töötleja, volitatud töötleja ja alltöötleja kontekstid;

1.2.3 PIMS-i toimivuse, privaatsuseesmärkide, kontrollimeetmete rakendamise staatuse, auditileidude, mittevastavuste, parandusmeetmete, juhtkonna läbivaatamise tegevuste ja täiustamistegevuste koondseire;

1.2.4 REG12-s säilitatav tõendusmaterjal ning REG01 kuni REG11-s säilitatav toetav lähtetõendusmaterjal.

1.3 Käesolev poliitika ei asenda muudes PIMS-i poliitikates määratletud operatiivse seire nõudeid. See kehtestab PIMS-i koondatud tulemuslikkuse hindamise, auditi, läbivaatamise ja täiustamise tsükli.

1.4 Käesoleva poliitika tähenduses on oluline PIMS-i mittevastavus rikkumine, mis mõjutab oluliselt PIMS-i kohaldamisala, privaatsuseesmärke, PII töötlemise vastutust, privaatsusriskide käsitlemist, isikuandmesubjekti õigusi, töötlemise turvalisust, volitatud töötleja või alltöötleja juhtimist, rikkumiseks valmisolekut, dokumenteeritud tõendusmaterjali terviklust, sertifitseerimise ulatust või sama nõude korduvat rikkumist 12-kuulise perioodi jooksul.

1.5 Käesoleva poliitika tähenduses on oluline muudatus mis tahes muudatus, mis mõjutab PIMS-i kohaldamisala, PII töötlemise eesmärke, PII kategooriaid, isikuandmesubjekti kategooriaid, töötlemiskohti, vastutava töötleja või volitatud töötleja rollide jaotust, süsteemiarhitektuuri, tarnija- või alltöötlejate kokkuleppeid, privaatsusriski profiili, kohaldatavaid õiguslikke või lepingulisi kohustusi, auditi ulatust, seiremeetodit või sertifitseerimise ulatust.

2. Eesmärk

2.1 Käesoleva poliitika eesmärk on tagada, et organisatsioon hindab PIMS-i toimivust, kontrollib PIMS-i vastavust, tuvastab mittevastavusi, parandab kontrollimeetmete nõrkusi ja täiustab PIMS-i pidevalt objektiivse tõendusmaterjali alusel.

2.2 Käesolev poliitika võimaldab organisatsioonil tõendada, et PIMS-i seire, audit, juhtkonna läbivaatamine ja täiustamistegevused on planeeritud, vajaduse korral sõltumatud, tõendusmaterjalil põhinevad, õigeaegsed ning jälgitavad vastutavate rollide ja kanooniliste tõendusmaterjali objektideni.

3. Eesmärgid

3.1 Käesoleva poliitika eesmärgid on:

3.1.1 määratleda PIMS-i koondatud seire- ja mõõtmisprotsess;

3.1.2 tagada, et privaatsuseesmärke ja PIMS-i kontrollimeetmete toimivust mõõdetakse dokumenteeritud tõendusmaterjali abil;

3.1.3 kehtestada PIMS-i jaoks riskipõhine siseauditi programm;

3.1.4 säilitada sõltumatus ja objektiivsus PIMS-i audititegevustes;

3.1.5 tagada, et juhtkonna läbivaatamisele esitatakse täielikud ja ajakohased PIMS-i toimivuse sisendid;

3.1.6 tagada, et mittevastavused registreeritakse, hinnatakse, parandatakse ja verifitseeritakse;

3.1.7 tagada, et parandusmeetmeid jälgitakse kuni lõpetamiseni ja nende tõhusus vaadatakse läbi;

3.1.8 tuvastada korduvad nõrkused ja täiustamisvõimalused;

3.1.9 toetada valmisolekut sertifitseerimiseks ja vastutuspõhist tõendusmaterjali haldust;

3.1.10 vältida seotud PIMS-i poliitikates juba määratletud operatiivmõõdikute dubleerimist.

4. Poliitika põhimõtted

4.1 PIMS-i seire- ja mõõtmisraamistik

4.1.1 [Both] Privacy Lead / PIMS Manager MUST määratlema PIMS-i koondatud seireprogrammi REG12-s enne PIMS-i esmast käitamist ja seejärel kord aastas.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST määratlema iga PIMS-i mõõdiku mõõtmismeetodi, sageduse, tõendusmaterjali allika, sihttaseme ja vastutava rolli REG12-s enne mõõtmistsükli algust.

4.1.3 [Both] Process Owner / Business Owner MUST esitama PII töötlemistoimingute seire sisendid REG02-st rollile Privacy Lead / PIMS Manager kord kvartalis.

4.1.4 [Both] Information Security Lead MUST esitama PII turbekontrollide staatuse sisendid REG03-st rollile Privacy Lead / PIMS Manager kord kvartalis.

4.1.5 [Both] Vendor / Procurement Owner MUST esitama volitatud töötleja, alltöötleja, kolmandate osapooltega jagamise ja tarnijakindluse staatuse sisendid REG08-st rollile Privacy Lead / PIMS Manager kord kvartalis.

4.1.6 [All] Incident Response Coordinator MUST esitama privaatsusintsidentide ja rikkumistrendide sisendid REG10-st rollile Privacy Lead / PIMS Manager kord kuus ning 10 tööpäeva jooksul pärast olulise intsidendi sulgemist.

4.1.7 [Both] Privacy Lead / PIMS Manager MUST koondama PIMS-i seiretulemused REG12-s kord kvartalis.

4.2 PIMS-i siseauditi programm

4.2.1 [All] Internal Audit / Compliance Reviewer MUST koostama riskipõhise PIMS-i siseauditi programmi REG12-s kord aastas enne esimest kavandatud PIMS-i audititsüklit.

4.2.2 [All] Internal Audit / Compliance Reviewer MUST määratlema iga PIMS-i auditi eesmärgi, kriteeriumid, ulatuse, meetodi, valimi aluse ja aruandlustähtaja REG12-s enne auditi välitööde algust.

4.2.3 [All] Internal Audit / Compliance Reviewer MUST registreerima audiitori sõltumatuse ja huvide konflikti kontrollid REG12-s enne iga audititöö määramist.

4.2.4 [All] Privacy Lead / PIMS Manager MUST tegema taotletud kontrollitud PIMS-i dokumenteeritud teabe ja registrite tõendusmaterjali REG12 kaudu kättesaadavaks 10 tööpäeva jooksul pärast heakskiidetud audititaotlust.

4.2.5 [Both] Internal Audit / Compliance Reviewer MUST testima kohaldatavate PIMS-i kontrollimeetmete rakendamise staatust REG03 alusel iga PIMS-i auditi käigus.

4.2.6 [Both] Internal Audit / Compliance Reviewer MUST registreerima valitud PII töötlemise tõendusmaterjali valimi REG12-s iga PIMS-i auditi käigus.

4.2.7 [All] Internal Audit / Compliance Reviewer MUST registreerima PIMS-i auditi tulemused REG12-s 15 tööpäeva jooksul pärast auditi lõpetamist.

4.2.8 [All] Privacy Lead / PIMS Manager MUST määrama aktsepteeritud PIMS-i auditileidude parandusmeetmete omanikud REG12-s 10 tööpäeva jooksul pärast auditi tulemuste aktsepteerimist.

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

9. Erandid

9.1 Seire, auditi ja täiustamise erandid

9.1.1 [All] Process Owner / Business Owner MUST taotlema iga erandit käesolevast poliitikast REG12-s enne kõrvalekalde tekkimist.

9.1.2 [All] Privacy Lead / PIMS Manager MUST hindama iga taotletud erandi mõju privaatsusele, sertifitseerimisele, auditile ja parandusmeetmetele REG12-s 10 tööpäeva jooksul pärast taotlust.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST registreerima nõuande REG12-s enne mis tahes erandi kinnitamist, mis mõjutab õiguslikke kohustusi, isikuandmesubjekti õigusi, DPIA kohustusi, kliendiauditi kohustusi või kõrge riskiga töötlemist.

9.1.4 [All] Top Management MUST kinnitama erandid, mis mõjutavad auditigraafiku täitmist, juhtkonna läbivaatamist, olulisi mittevastavusi, sertifitseerimise ulatust või kõrge riskiga töötlemist, REG12-s enne erandi jõustumist.

9.1.5 [All] Privacy Lead / PIMS Manager MUST määrama iga kinnitatud seire-, auditi- või täiustamiserandi aegumiskuupäeva REG12-s, mis ei ületa 90 päeva.

9.1.6 [All] Privacy Lead / PIMS Manager MUST sulgema või uuesti hindama iga seire-, auditi- või täiustamiserandi REG12-s viie tööpäeva jooksul pärast aegumist.

10. Rakendamine

10.1 Seire, auditi ja täiustamise nõuete rakendamine

10.1.1 [All] Privacy Lead / PIMS Manager MUST registreerima vahele jäänud seiretsükli, vahele jäänud PIMS-i auditi, tähtaja ületanud juhtkonna läbivaatamise, puuduva audititõenduse, tähtaja ületanud parandusmeetme või tähtaja ületanud täiustamistegevuse mittevastavusena REG12-s viie tööpäeva jooksul pärast tuvastamist.

10.1.2 [All] Internal Audit / Compliance Reviewer MUST registreerima auditileiu raskusastme REG12-s enne auditiaruande väljastamist.

10.1.3 [All] Top Management MUST nõudma iga olulise PIMS-i mittevastavuse parandusmeedet REG12-s 10 tööpäeva jooksul pärast eskaleerimist.

10.1.4 [All] Process Owner / Business Owner MUST takistama kõrge riskiga töötlemise tootmiskeskkonda kasutuselevõttu või välise kindluse andmise esitamist, kui nõutava parandusmeetme tõendusmaterjal puudub REG12-st enne tootmiskeskkonda kasutuselevõttu või esitamist.

10.1.5 [All] Privacy Lead / PIMS Manager MUST eskaleerima korduvad vahele jäänud seire- või parandusmeetmete tähtajad rollile Top Management REG12-s viie tööpäeva jooksul pärast teist esinemist 12-kuulise perioodi jooksul.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST verifitseerima rakendamistegevuse sulgemise REG12-s järgmisel kavandatud auditil või 60 päeva jooksul pärast teatatud sulgemist, olenevalt sellest, kumb saabub varem.

11. Läbivaatamine ja ajakohastamine

11.1 Poliitika läbivaatamine ja ajakohastamine

11.1.1 [All] Privacy Lead / PIMS Manager MUST vaatama käesoleva poliitika REG12-s läbi kord aastas ning 30 päeva jooksul pärast olulist muudatust PIMS-i seire, auditi, juhtkonna läbivaatamise, parandusmeetmete või sertifitseerimisnõuetes.

11.1.2 [All] Internal Audit / Compliance Reviewer MUST vaatama PIMS-i auditi programmi tõhususe REG12-s läbi kord aastas pärast PIMS-i tegevusaasta viimast kavandatud auditit.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager MUST ajakohastama REG01 ja REG03 15 tööpäeva jooksul pärast käesoleva poliitika kinnitatud muudatusi, mis muudavad PIMS-i kohaldamisala või kontrollimeetme kohaldatavust.

11.1.6 [All] Privacy Lead / PIMS Manager MUST registreerima käesoleva poliitika kinnitatud muudatuste teavitamise REG11-s 30 päeva jooksul pärast avaldamist.

12. Seotud poliitikad

12.1 Käesolevat poliitikat toetavad järgmised seotud poliitikad:

12.2 PII01 - Privaatsusteabe haldussüsteemi poliitika

12.3 PII02 - Privaatsusrollide, vastutuste ja vastutuse poliitika

12.4 PII03 - PII töötlemise registri 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 andmekaitse 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 töötlejate, alltöötlejate ja kolmandate osapoolte privaatsushalduse poliitika

12.14 PII13 - Rahvusvahelise PII edastamise poliitika

12.15 PII14 - PII turbe ja juurdepääsukontrolli poliitika

12.16 PII15 - PII intsidendi- ja rikkumishalduse poliitika

12.17 PII16 - Privaatsuskoolituse, teadlikkuse ja pädevuse poliitika

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

13. Viitestandardid ja raamistikud

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Vastendatud PIMS-i eesmärkide ja PIMS-i toimivusmõõdikute määratlemisele, mõõtmisele, aruandlusele ja läbivaatamisele. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Vastendatud dokumenteeritud teabe haldamisele seiretulemuste, auditiprogrammide, audititulemuste, juhtkonna läbivaatamise tõendusmaterjali, mittevastavuste, parandusmeetmete ja täiustamistegevuste kohta. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Vastendatud kavandatud PIMS-i seire-, auditi-, parandusmeetmete ja täiustamistsükli käitamisele PIMS-i tegevusohje osana. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Vastendatud seiratava ja mõõdetava määratlemisele, seiretulemuste koondamisele, PIMS-i toimivuse hindamisele ning mõõtmistõendite säilitamisele. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Vastendatud siseauditi programmi haldamisele, auditi planeerimisele, audiitori sõltumatuse kontrollidele, tõendusmaterjali valimitele, audititulemustele ja auditileidude järeltegevustele. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Vastendatud juhtkonna läbivaatamise planeerimisele, PIMS-i toimivuse läbivaatamisele, auditi- ja parandusmeetmete trendide läbivaatamisele, väljundite kinnitamisele ja ressursiotsustele. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Vastendatud PIMS-i sobivuse, piisavuse ja tõhususe pideva täiustamise võimaluste tuvastamisele, kinnitamisele, rakendamisele ja jälgimisele. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Vastendatud mittevastavuste registreerimisele, algpõhjuse analüüsile, parandusmeetmete planeerimisele, parandusmeetmete rakendamisele, tõhususe verifitseerimisele, eskaleerimisele ja rakendamisele. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Vastendatud vastutava töötleja töötlemiskirjetele, mida kasutatakse seire, auditivalimi ja töötlemisregistri ajakohasuse mõõdikute tõendusallikatena. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Vastendatud volitatud töötleja lepingu, kliendiauditi, kindluse andmise vastuse ja volitatud töötleja koostöö tõendusmaterjalile, mida jälgitakse tarnija- ja kliendikindluse protsesside kaudu. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Vastendatud seire, auditi, juhtkonna läbivaatamise, parandusmeetmete ja pideva täiustamise vastutuse tõendusmaterjalile. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Vastendatud vastutava töötleja juhtimismeetmetele, tõhususe läbivaatamisele, juhtkonna läbivaatamisele, parandusmeetmetele ja dokumenteeritud täiustamistõenditele. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Vastendatud volitatud töötleja, alltöötleja, kliendiauditi, kolmanda osapoole kindluse ja tarnija koostöö tõendusmaterjalile. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Vastendatud töötlemiskirjetele, mida kasutatakse seire, auditivalimi, tõendusmaterjali objektide täielikkuse ja töötlemisregistri ajakohasuse tõendusmaterjalina. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Vastendatud PII turbekontrollide staatuse seirele ja hindamisele, tehniliste kontrollimeetmete tõendusmaterjalile ning turbega seotud tõhususe tõendusmaterjalile. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Vastendatud Data Protection Officer / Privacy Advisor privaatsusnõuannetele, seire tähelepanekutele, auditi toetamisele ja privaatsusnõuetele vastavuse trendide läbivaatamisele, kui kohaldatav. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Vastendatud privaatsusnõuetele vastavuse kontrollimisele, sise- või sõltumatutele auditite, sisekontrollidele, järelevalvemehhanismidele ja privaatsusriskide hindamise tõendusmaterjalile. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Vastendatud PII-ga seotud infoturbe sõltumatule läbivaatamisele, poliitikate ja standardite vastavusele ning PII kaitse tehnilisele vastavuse läbivaatamisele. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Vastendatud infoturbe seire- ja hindamissisenditele, mis toetavad PIMS-i toimivuse mõõtmist ja PII turbekontrollide staatust. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Vastendatud ISMS-i siseauditi toele PIMS-i auditi planeerimisel, audititõendusmaterjali, audititulemuste ja auditi programmi lõpetamise osas. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Vastendatud juhtkonna läbivaatamise sisenditele ja väljunditele integreeritud PIMS-i ja infoturbe toimivuse järelevalves. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Vastendatud PIMS-i ja toetava infoturbe kontrollikeskkonna pidevale täiustamisele. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Vastendatud mittevastavuste käsitlemisele, parandusmeetmete planeerimisele, parandusmeetmete rakendamisele ja tõhususe verifitseerimisele. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Vastendatud sõltumatule läbivaatamisele, audiitori sõltumatuse kontrollidele, audititõendusmaterjali testimisele ja parandusmeetmete tõhususe sõltumatule verifitseerimisele. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Vastendatud PIMS-i ja infoturbe poliitikate vastavuse läbivaatamisele, kontrollimeetmete rakendamise staatusele ning standarditele vastavuse tõendusmaterjalile. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Vastendatud auditi põhimõtetele, auditiprogrammi juhtimisele, auditi läbiviimisele, tõendusmaterjalil põhinevale auditiaruandlusele, auditi järeltegevustele ja PIMS-i audiitorite pädevusootustele. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].