					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: PII18					Dokumenta nosaukums: **PIMS uzraudzības, audita un uzlabošanas politika**						
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:						
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/kontrole/pants	Piemērojamība	Aptvēruma veids	Piezīme
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Privātuma mērķu mērīšana
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentēta informācija par uzraudzību, auditu un uzlabošanu
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Darbības plānošanas un kontroles uzraudzība
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Uzraudzība, mērīšana, analīze un izvērtēšana
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Iekšējais audits
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Vadības pārskatīšana
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Nepārtraukta uzlabošana
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neatbilstība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Pārziņa apstrādes ieraksti, ko izmanto auditam
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Apstrādātāja līguma un sadarbības auditā pierādījumi
GDPR	Article 5(2)	Controller	Supporting	Pārskatatbildības pierādījumi
GDPR	Article 24	Controller	Supporting	Pārziņa pasākumi un efektivitātes pārskatīšana
GDPR	Article 28	Both	Supporting	Apstrādātāja audita un sadarbības pārvaldība
GDPR	Article 30	Both	Supporting	Apstrādes ieraksti, ko izmanto auditam

GDPR	Article 32	Both	Supporting	Drošības pasākumu testēšana un izvērtēšana
GDPR	Article 39	Conditional	Supporting	Datu aizsardzības speciālista uzraudzība un konsultācijas par auditu, ja piemērojams
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privātuma atbilstība, audits un neatkarīga uzraudzība
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	PII aizsardzības pārskatīšana un atbilstības pārbaudes
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Informācijas drošības uzraudzība un izvērtēšana
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS iekšējā audita atbalsts
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS vadības pārskatīšanas atbalsts
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS nepārtrauktas uzlabošanas atbalsts
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS neatbilstību un korektīvo darbību atbalsts
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Neatkarīga informācijas drošības pārskatīšana
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Politiku un standartu atbilstības pārskatīšana
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Pārvaldības sistēmu audita principi, programma,

				norise un kompetence

1. Piemērošanas joma

1.1 Šī politika nosaka organizācijas prasības PIMS uzraudzībai, mērīšanai, analīzei, izvērtēšanai, iekšējam auditam, vadības pārskatīšanai, neatbilstību pārvaldībai, korektīvajām darbībām un nepārtrauktai uzlabošanai.

1.2 Šī politika attiecas uz tālāk norādīto:

1.2.1 visiem PIMS procesiem, kontroles pasākumiem, politikām, reģistriem, pierādījumu objektiem, sistēmām, piegādātājiem, apstrādātājiem, apakšapstrādātājiem un datu koplietošanas kārtībām PIMS darbības jomā;

1.2.2 organizācijas pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem;

1.2.3 PIMS veiktspējas, privātuma mērķu, kontroles pasākumu ieviešanas statusa, audita konstatējumu, neatbilstību, korektīvo darbību, vadības pārskatīšanas darbību un uzlabošanas darbību konsolidētu uzraudzību;

1.2.4 pierādījumiem, kas glabāti REG12, un atbalstošajiem avota pierādījumiem, kas glabāti REG01 līdz REG11.

1.3 Šī politika neaizstāj citās PIMS politikās noteiktās operatīvās uzraudzības prasības. Tā nosaka PIMS konsolidēto veiktspējas izvērtēšanas, audita, pārskatīšanas un uzlabošanas ciklu.

1.4 Šīs politikas vajadzībām būtiska PIMS neatbilstība nozīmē kļūmi, kas būtiski ietekmē PIMS darbības jomu, privātuma mērķus, PII apstrādes pārskatatbildību, privātuma riska apstrādi, datu subjektu tiesības, apstrādes drošību, apstrādātāju vai apakšapstrādātāju pārvaldību, gatavību pārkāpumiem, dokumentēto pierādījumu integritāti, sertifikācijas darbības jomu vai atkārtotu tās pašas prasības neizpildi 12 mēnešu periodā.

1.5 Šīs politikas vajadzībām būtiska izmaiņa nozīmē jebkuru izmaiņu, kas ietekmē PIMS darbības jomu, PII apstrādes nolūkus, PII kategorijas, datu subjektu kategorijas, apstrādes vietas, pārziņa vai apstrādātāja lomu sadalījumu, sistēmas arhitektūru, piegādātāju vai apakšapstrādātāju kārtību, privātuma riska profilu, piemērojamos juridiskos vai līgumiskos pienākumus, audita darbības jomu, uzraudzības metodi vai sertifikācijas darbības jomu.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka organizācija izvērtē PIMS veiktspēju, pārbauda PIMS atbilstību, identificē neatbilstības, labo kontroles pasākumu vājās vietas un nepārtraukti uzlabo PIMS, izmantojot objektīvus pierādījumus.

2.2 Šī politika ļauj organizācijai pierādīt, ka PIMS uzraudzības, audita, vadības pārskatīšanas un uzlabošanas darbības ir plānotas, neatkarīgas, ja tas nepieciešams, balstītas pierādījumos, savlaicīgas un izsekojamas līdz atbildīgajām lomām un kanoniskajiem pierādījumu objektiem.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 noteikt konsolidētu PIMS uzraudzības un mērīšanas procesu;

3.1.2 nodrošināt, ka privātuma mērķi un PIMS kontroles pasākumu veiktspēja tiek mērīti, izmantojot dokumentētus pierādījumus;

3.1.3 izveidot uz risku balstītu PIMS iekšējā audita programmu;

3.1.4 saglabāt neatkarību un objektivitāti PIMS audita darbībās;

3.1.5 nodrošināt, ka vadības pārskatīšanai tiek sniegti pilnīgi un aktuāli PIMS veiktspējas ievaddati;

3.1.6 nodrošināt, ka neatbilstības tiek reģistrētas, izvērtētas, labotas un verificētas;

3.1.7 nodrošināt, ka korektīvās darbības tiek izsekotas līdz slēgšanai un pārskatītas attiecībā uz efektivitāti;

3.1.8 identificēt atkārtotas vājās vietas un uzlabošanas iespējas;

3.1.9 atbalstīt gatavību sertifikācijai un pārskatatbildīgu pierādījumu pārvaldību;

3.1.10 nepieļaut operatīvo metriku dublēšanu, ja tās jau noteiktas saistītajās PIMS politikās.

4. Politikas paziņojumi

4.1 PIMS uzraudzības un mērīšanas ietvars

4.1.1 [Both] Privacy Lead / PIMS Manager ir jānosaka konsolidētā PIMS uzraudzības programma REG12 pirms sākotnējās PIMS darbības un pēc tam reizi gadā.

4.1.2 [Both] Privacy Lead / PIMS Manager ir jānosaka mērīšanas metode, biežums, pierādījumu avots, mērķrādītājs un atbildīgā loma katrai PIMS metrikai REG12 pirms mērīšanas cikla sākuma.

4.1.3 [Both] Process Owner / Business Owner reizi ceturksnī ir jāsniedz Privacy Lead / PIMS Manager PII apstrādes darbību uzraudzības ievaddati no REG02.

4.1.4 [Both] Information Security Lead reizi ceturksnī ir jāsniedz Privacy Lead / PIMS Manager PII drošības kontroles pasākumu statusa ievaddati no REG03.

4.1.5 [Both] Vendor / Procurement Owner reizi ceturksnī ir jāsniedz Privacy Lead / PIMS Manager apstrādātāju, apakšapstrādātāju, trešo pušu koplietošanas un piegādātāju apliecinājuma statusa ievaddati no REG08.

4.1.6 [All] Incident Response Coordinator reizi mēnesī un 10 darba dienu laikā pēc būtiska incidenta slēgšanas ir jāsniedz Privacy Lead / PIMS Manager privātuma incidentu un pārkāpumu tendenču ievaddati no REG10.

4.1.7 [Both] Privacy Lead / PIMS Manager reizi ceturksnī ir jākonsolidē PIMS uzraudzības rezultāti REG12.

4.2 PIMS iekšējā audita programma

4.2.1 [All] Internal Audit / Compliance Reviewer reizi gadā pirms pirmā plānotā PIMS audita cikla ir jāsagatavo uz risku balstīta PIMS iekšējā audita programma REG12.

4.2.2 [All] Internal Audit / Compliance Reviewer pirms audita darba uz vietas sākuma ir jānosaka katra PIMS audita mērķis, kritēriji, darbības joma, metode, izlases pamats un ziņošanas termiņš REG12.

4.2.3 [All] Internal Audit / Compliance Reviewer pirms katra audita uzdevuma ir jāreģistrē auditoru neatkarības un interešu konflikta pārbaudes REG12.

4.2.4 [All] Privacy Lead / PIMS Manager 10 darba dienu laikā pēc apstiprināta audita pieprasījuma ir jānodrošina pieprasītās kontrolētās PIMS dokumentētās informācijas un reģistru pierādījumu pieejamība, izmantojot REG12.

4.2.5 [Both] Internal Audit / Compliance Reviewer katra PIMS audita laikā ir jāpārbauda piemērojamo PIMS kontroles pasākumu ieviešanas statuss pret REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer katra PIMS audita laikā ir jāreģistrē atlasītā PII apstrādes pierādījumu izlase REG12.

4.2.7 [All] Internal Audit / Compliance Reviewer 15 darba dienu laikā pēc audita pabeigšanas ir jāreģistrē PIMS audita rezultāti REG12.

4.2.8 [All] Privacy Lead / PIMS Manager 10 darba dienu laikā pēc audita rezultātu pieņemšanas ir jāpiešķir korektīvo darbību īpašnieki pieņemtajiem PIMS audita konstatējumiem REG12.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Izņēmumi

9.1 Uzraudzības, audita un uzlabošanas izņēmumi

9.1.1 [All] Process Owner / Business Owner pirms atkāpes rašanās ir jāpieprasa jebkurš izņēmums no šīs politikas REG12.

9.1.2 [All] Privacy Lead / PIMS Manager 10 darba dienu laikā pēc pieprasījuma ir jāizvērtē katra pieprasītā izņēmuma ietekme uz privātumu, sertifikāciju, auditu un korektīvajām darbībām REG12.

9.1.3 [All] Data Protection Officer / Privacy Advisor pirms jebkura izņēmuma apstiprināšanas, kas ietekmē juridiskos pienākumus, datu subjektu tiesības, DPIA saistības, klientu audita pienākumus vai augsta riska apstrādi, ir jāreģistrē konsultācija REG12.

9.1.4 [All] Top Management pirms izņēmuma stāšanās spēkā REG12 ir jāapstiprina izņēmumi, kas ietekmē audita grafika izpildi, vadības pārskatīšanu, būtiskas neatbilstības, sertifikācijas darbības jomu vai augsta riska apstrādi.

9.1.5 [All] Privacy Lead / PIMS Manager katram apstiprinātam uzraudzības, audita vai uzlabošanas izņēmumam REG12 ir jānosaka beigu datums, kas nepārsniedz 90 dienas.

9.1.6 [All] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc termiņa beigām ir jāslēdz vai atkārtoti jāizvērtē katrs uzraudzības, audita vai uzlabošanas izņēmums REG12.

10. Piemērošana

10.1 Uzraudzības, audita un uzlabošanas prasību piemērošana

10.1.1 [All] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc identificēšanas ir jāreģistrē nokavēts uzraudzības cikls, nokavēts PIMS audits, kavēta vadības pārskatīšana, trūkstoši audita pierādījumi, kavēta korektīvā darbība vai kavēta uzlabošanas darbība kā neatbilstība REG12.

10.1.2 [All] Internal Audit / Compliance Reviewer pirms audita pārskata izdošanas ir jāreģistrē audita konstatējuma smaguma pakāpe REG12.

10.1.3 [All] Top Management 10 darba dienu laikā pēc eskalācijas ir jāpieprasa korektīvā darbība par katru būtisku PIMS neatbilstību REG12.

10.1.4 [All] Process Owner / Business Owner ir jānovērš nodošana ražošanas vidē vai ārēja apliecinājuma iesniegšana augsta riska apstrādei, ja nepieciešamie korektīvās darbības pierādījumi pirms nodošanas ražošanas vidē vai iesniegšanas nav pieejami REG12.

10.1.5 [All] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc otrā gadījuma 12 mēnešu periodā ir jāeskalē atkārtoti nokavēti uzraudzības vai korektīvo darbību termiņi Top Management REG12.

10.1.6 [All] Internal Audit / Compliance Reviewer nākamajā plānotajā auditā vai 60 dienu laikā pēc paziņotās slēgšanas, atkarībā no tā, kas notiek agrāk, ir jāverificē piemērošanas darbības slēgšana REG12.

11. Pārskatīšana un uzturēšana

11.1 Politikas pārskatīšana un uzturēšana

11.1.1 [All] Privacy Lead / PIMS Manager reizi gadā un 30 dienu laikā pēc būtiskām izmaiņām PIMS uzraudzības, audita, vadības pārskatīšanas, korektīvo darbību vai sertifikācijas prasībās ir jāpārskata šī politika REG12.

11.1.2 [All] Internal Audit / Compliance Reviewer reizi gadā pēc pēdējā plānotā audita PIMS darbības gadā ir jāpārskata PIMS audita programmas efektivitāte REG12.

11.1.3 [All] Data Protection Officer / Privacy Advisor pirms apstiprināšanas ir jāpārskata privātuma ziņā nozīmīgas izmaiņas šajā politikā REG12.

11.1.4 [All] Top Management pirms publicēšanas ir jāapstiprina būtiskas izmaiņas šajā politikā REG12.

11.1.5 [All] Privacy Lead / PIMS Manager 15 darba dienu laikā pēc apstiprinātām izmaiņām šajā politikā, kas maina PIMS darbības jomu vai kontroles pasākumu piemērojamību, ir jāatjaunina REG01 un REG03.

11.1.6 [All] Privacy Lead / PIMS Manager 30 dienu laikā pēc publicēšanas ir jāreģistrē apstiprināto izmaiņu paziņošana par šo politiku REG11.

12. Saistītās politikas

12.1 Šo politiku atbalsta šādas saistītās politikas:

12.2 PII01 - Privātuma informācijas pārvaldības sistēmas politika

12.3 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.4 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika

12.5 PII04 - Privātuma paziņojuma un pārredzamības politika

12.6 PII05 - Piekrišanas un preferenču pārvaldības politika

12.7 PII06 - Datu subjektu tiesību pārvaldības politika

12.8 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.9 PII08 - Integrētās datu aizsardzības un datu aizsardzības pēc noklusējuma politika

12.10 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika

12.11 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika

12.12 PII11 - PII precizitātes un kvalitātes politika

12.13 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika

12.14 PII13 - Starptautiskas PII nosūtīšanas politika

12.15 PII14 - PII drošības un piekļuves kontroles politika

12.16 PII15 - PII incidentu un pārkāpumu pārvaldības politika

12.17 PII16 - Privātuma apmācības, informētības un kompetences politika

12.18 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir kartēta uz tālāk norādītajiem standartiem un regulējumu. Kartējums skaidro, kā politika atbalsta norādītās prasības, un identificē iekšējos punktus, kas tās ievieš vai atbalsta.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Kartēts uz PIMS mērķu un PIMS veiktspējas metriku noteikšanu, mērīšanu, ziņošanu un pārskatīšanu. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Kartēts uz dokumentētas informācijas uzturēšanu par uzraudzības rezultātiem, audita programmām, audita rezultātiem, vadības pārskatīšanas pierādījumiem, neatbilstībām, korektīvajām darbībām un uzlabošanas darbībām. 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** - Kartēts uz plānotā PIMS uzraudzības, audita, korektīvo darbību un uzlabošanas cikla darbību kā PIMS darbības kontroles daļu. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Kartēts uz uzraugāmā un mērāmā noteikšanu, uzraudzības rezultātu konsolidēšanu, PIMS veiktspējas izvērtēšanu un mērījumu pierādījumu uzturēšanu. 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** - Kartēts uz iekšējā audita programmas uzturēšanu, audita plānošanu, auditoru neatkarības pārbaudēm, pierādījumu izlasi, audita rezultātiem un audita konstatējumu pēckontroli. 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** - Kartēts uz vadības pārskatīšanas plānošanu, PIMS veiktspējas pārskatīšanu, audita un korektīvo darbību tendenču pārskatīšanu, izvaddatu apstiprināšanu un resursu lēmumiem. 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** - Kartēts uz nepārtrauktas uzlabošanas iespēju identificēšanu, apstiprināšanu, ieviešanu un izsekošanu attiecībā uz PIMS piemērotību, pietiekamību un efektivitāti. 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** - Kartēts uz neatbilstību reģistrēšanu, pamatcēloņa analīzi, korektīvo darbību plānošanu, korektīvo darbību ieviešanu, efektivitātes verifikāciju, eskalāciju un piemērošanu. 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** - Kartēts uz pārziņa apstrādes ierakstiem, ko izmanto kā pierādījumu avotus uzraudzībai, audita izlasei un apstrādes uzskaites aktualitātes metrikām. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Kartēts uz apstrādātāja līguma, klienta audita, apliecinājuma atbildes un apstrādātāja sadarbības pierādījumiem, ko izseko piegādātāju un klientu apliecinājuma procesos. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartēts uz pārskatatbildības pierādījumiem par uzraudzību, auditu, vadības pārskatīšanu, korektīvajām darbībām un nepārtrauktu uzlabošanu. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Kartēts uz pārziņa pārvaldības pasākumiem, efektivitātes pārskatīšanu, vadības pārskatīšanu, korektīvajām darbībām un dokumentētiem uzlabošanas pierādījumiem. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Kartēts uz apstrādātāju, apakšapstrādātāju, klienta audita, trešās puses apliecinājuma un piegādātāju sadarbības pierādījumiem. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Kartēts uz apstrādes ierakstiem, ko izmanto kā uzraudzības, audita izlases, pierādījumu objektu pilnīguma un apstrādes uzskaites aktualitātes pierādījumus. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Kartēts uz PII drošības kontroles pasākumu statusa, tehnisko kontroles pasākumu pierādījumu un ar drošību saistīto efektivitātes pierādījumu uzraudzību un izvērtēšanu. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Kartēts uz privātuma konsultācijām, uzraudzības novērojumiem, audita atbalstu un privātuma atbilstības tendenču pārskatīšanu, ko veic Data Protection Officer / Privacy Advisor, ja piemērojams. 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** - Kartēts uz privātuma atbilstības verifikāciju, iekšējiem vai neatkarīgiem auditiem, iekšējiem kontroles pasākumiem, uzraudzības mehānismiem un privātuma risku izvērtēšanas pierādījumiem. 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** - Kartēts uz neatkarīgu ar PII saistītas informācijas drošības pārskatīšanu, atbilstību politikām un standartiem un tehnisko atbilstības pārskatīšanu PII aizsardzībai. 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** - Kartēts uz informācijas drošības uzraudzības un izvērtēšanas ievaddatiem, kas atbalsta PIMS veiktspējas mērīšanu un PII drošības kontroles pasākumu statusu. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Kartēts uz ISMS iekšējā audita atbalstu PIMS audita plānošanai, audita pierādījumiem, audita rezultātiem un audita programmas pabeigšanai. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Kartēts uz vadības pārskatīšanas ievaddatiem un izvaddatiem integrētai PIMS un informācijas drošības veiktspējas pārraudzībai. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Kartēts uz PIMS un atbalstošās informācijas drošības kontroles vides nepārtrauktu uzlabošanu. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Kartēts uz neatbilstību pārvaldību, korektīvo darbību plānošanu, korektīvo darbību ieviešanu un efektivitātes verifikāciju. 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 - Kartēts uz neatkarīgu pārskatīšanu, auditoru neatkarības pārbaudēm, audita pierādījumu testēšanu un korektīvo darbību efektivitātes neatkarīgu verifikāciju. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Kartēts uz PIMS un informācijas drošības politiku atbilstības pārskatīšanu, kontroles pasākumu ieviešanas statusu un standartu atbilstības pierādījumiem. 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** - Kartēts uz audita principiem, audita programmas pārvaldību, audita norisi, pierādījumos balstītu audita ziņošanu, audita pēckontroli un auditoru kompetences prasībām PIMS auditos. 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].