					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII17					Dokumenta nosaukums: **PIMS dokumentētās informācijas un pierādījumu pārvaldības 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	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA dokumentētā informācija
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS dokumentētā informācija
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Darbības pierādījumu kontrole
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Uzraudzības pierādījumi
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Audita pierādījumi
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vadības pārskata pierādījumi
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neatbilstību un korektīvo darbību pierādījumi
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Pārziņa apstrādes ieraksti
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Apstrādātāja vienošanās un norādījumu pierādījumi
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Ierakstu aizsardzība
GDPR	Article 5(2)	Controller	Supporting	Pārskatatbildības pierādījumi
GDPR	Article 24	Controller	Supporting	Pārziņa pasākumi un pierādījumi
GDPR	Article 28	Both	Supporting	Apstrādātāja dokumentācija
GDPR	Article 30	Both	Supporting	Apstrādes ieraksti
GDPR	Article 32	Both	Supporting	Pierādījumu aizsardzība
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privātuma atbilstības pierādījumi
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Ierakstu aizsardzība

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Dokumentētās informācijas kontrole
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Ierakstu aizsardzība
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Privātuma un PII aizsardzība

1. Piemērošanas joma

1.1 Šī politika nosaka obligātās prasības PIMS dokumentētās informācijas izveidei, apstiprināšanai, versiju pārvaldībai, aizsardzībai, glabāšanai, izgūšanai, tulkošanai, atsaukšanai un pierādīšanai.

1.2 Šī politika attiecas uz PIMS politikām, reģistriem, dokumentētiem apstiprinājumiem, pierādījumu ierakstiem, audita pierādījumiem, vadības pārskata ierakstiem, korektīvo darbību pierādījumiem un kontrolētiem tulkojumiem, ko izmanto PIMS atbilstības pierādīšanai.

1.3 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem.

1.4 Šī politika neveido atsevišķu dokumentu kontroles reģistru. Dokumentētās informācijas kontroles pierādījumi tiek uzturēti, izmantojot kanoniskos PIMS pierādījumu objektus no REG01 līdz REG12, savukārt REG03 un REG12 tiek izmantoti kontroles pasākumu piemērojamības, audita, neatbilstību, korektīvo darbību un uzlabojumu pierādījumiem.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka PIMS dokumentētā informācija ir precīza, kontrolēta, pieejama pilnvarotiem lietotājiem, aizsargāta pret neatļautām izmaiņām vai izpaušanu, saglabāta auditējamības nodrošināšanai un atsaukta, kad tā kļūst novecojusi.

2.2 Šī politika atbalsta gatavību sertifikācijai, nodrošinot, ka pierādījumus, kas nepieciešami PIMS atbilstības apliecināšanai, var atrast, verificēt, izgūt un sasaistīt ar piemērojamām politikām, kontroles pasākumiem, apstrādes darbībām, riskiem, auditiem un korektīvajām darbībām.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 noteikt PIMS dokumentētās informācijas kontroles prasības;

3.1.2 uzturēt pierādījumu integritāti visos objektos no REG01 līdz REG12;

3.1.3 nodrošināt politiku un pierādījumu apstiprināšanas izsekojamību;

3.1.4 nodrošināt, ka versiju vēsture un lēmumi par atsaukšanu ir dokumentēti;

3.1.5 sasaistīt PIMS pierādījumus ar Piemērojamības paziņojumu un politiku kartējumiem;

3.1.6 kontrolēt piekļuvi PIMS dokumentiem un pierādījumu ierakstiem;

3.1.7 atbalstīt daudzvalodu politiku un pierādījumu versiju kontroli;

3.1.8 nodrošināt savlaicīgu audita pierādījumu izgūšanu;

3.1.9 novērst nevajadzīgu dokumentu kontroles birokrātiju;

3.1.10 saglabāt auditam gatavus ierakstus sertifikācijai, klientu apliecinājumam un nepārtrauktai uzlabošanai.

4. Politikas paziņojumi

4.1 PIMS dokumentētās informācijas kontrole

4.1.1 [All] Privacy Lead / PIMS Manager jāuztur PIMS dokumentētās informācijas indekss REG12 pirms sākotnējās PIMS publicēšanas un pēc tam reizi ceturksnī.

4.1.2 [All] Process Owner / Business Owner jāidentificē dokumentētā informācija, kas nepieciešama katrai tā pārziņā esošai PII apstrādes darbībai REG02 pirms apstrādes darbības sākšanas un pēc tam reizi gadā.

4.1.3 [All] Privacy Lead / PIMS Manager jāsasaista piemērojamās PIMS politikas, kontroles pasākumi un pierādījumu pienākumi ar REG03 pirms katra politikas laidiena un 15 darba dienu laikā pēc jebkādām būtiskām izmaiņām kontroles pasākumu piemērojamībā.

4.1.4 [All] Privacy Lead / PIMS Manager jāpiešķir piekļuves līmenis un pierādījumu sensitivitātes klasifikācija katrai PIMS dokumentētās informācijas kategorijai REG12 pirms attiecīgās kategorijas izmantošanas.

4.2 Izveide, apstiprināšana, versiju pārvaldība un publicēšana

4.2.1 [All] Privacy Lead / PIMS Manager jāpiešķir dokumenta identifikators, īpašnieks, versijas numurs, apstiprināšanas statuss, spēkā stāšanās datums un pārskatīšanas datums REG12 pirms PIMS dokumentētās informācijas publicēšanas.

4.2.2 [All] Top Management jāapstiprina PIMS pamatpolitikas un būtiskas politiku izmaiņas REG12 pirms publicēšanas.

4.2.3 [All] Privacy Lead / PIMS Manager jāapstiprina PIMS pierādījumu veidnes vai iegultās reģistra sadaļas REG12 pirms darbības izmantošanas.

4.2.4 [All] Privacy Lead / PIMS Manager jāreģistrē versiju vēsture un izmaiņu pamatojums REG12 pirms atjauninātas PIMS dokumentētās informācijas izlaišanas.

4.2.5 [All] Privacy Lead / PIMS Manager jāreģistrē apstiprināto PIMS dokumentētās informācijas izmaiņu paziņošana REG11 30 dienu laikā pēc publicēšanas.

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

9. Izņēmumi

9.1.1 [All] Process Owner / Business Owner jāpieprasa dokumentētās informācijas vai pierādījumu kontroles izņēmumi REG12 pirms atkāpšanās no šīs politikas.

9.1.2 [All] Privacy Lead / PIMS Manager jāizvērtē katrs dokumentētās informācijas vai pierādījumu kontroles izņēmums REG12 10 darba dienu laikā pēc pieprasījuma.

9.1.3 [All] Data Protection Officer / Privacy Advisor jāreģistrē konsultācija REG12 pirms jebkāda izņēmuma apstiprināšanas, kas saistīts ar PII pierādījumu izpaušanu, tulkojuma neatbilstību, glabāšanas konfliktu vai audita pierādījumu ierobežojumu.

9.1.4 [All] Top Management jāapstiprina dokumentētās informācijas izņēmumi, kas pārsniedz 30 dienas vai ietekmē sertifikāciju, augsta riska apstrādi vai ārēju apliecinājumu, REG12 pirms izņēmuma stāšanās spēkā.

9.1.5 [All] Privacy Lead / PIMS Manager katram apstiprinātam dokumentētās informācijas vai pierādījumu kontroles izņēmumam REG12 jānosaka termiņa beigu datums, kas nepārsniedz 90 dienas.

9.1.6 [All] Privacy Lead / PIMS Manager jāslēdz vai atkārtoti jāizvērtē katrs dokumentētās informācijas vai pierādījumu kontroles izņēmums REG12 piecu darba dienu laikā pēc termiņa beigām.

10. Piemērošana

10.1.1 [All] Privacy Lead / PIMS Manager piecu darba dienu laikā pēc identificēšanas jāreģistrē trūkstoša, neprecīza, nekontrolēta, novecojusi vai neizgūstama PIMS dokumentētā informācija kā neatbilstība REG12.

10.1.2 [All] Privacy Lead / PIMS Manager jānovērš PIMS dokumentētās informācijas publicēšana, ja REG12 trūkst nepieciešamā apstiprinājuma, versijas, īpašnieka vai spēkā stāšanās datuma pierādījumu.

10.1.3 [All] Process Owner / Business Owner jānovērš apstrādes pierādījumu iesniegšana auditam, ja REG02 trūkst nepieciešamā īpašnieka, datuma, statusa vai apstiprinājuma pierādījumu.

10.1.4 [All] System Owner / Application Owner jānoņem neatļauta piekļuve PIMS dokumentētās informācijas repozitorijiem un jāreģistrē noņemšana REG12 vienas darba dienas laikā pēc identificēšanas.

10.1.5 [All] Internal Audit / Compliance Reviewer nākamajā plānotajā auditā vai 60 dienu laikā pēc slēgšanas, atkarībā no tā, kas notiek agrāk, REG12 jāverificē korektīvo darbību efektivitāte attiecībā uz dokumentētās informācijas neatbilstībām.

11. Pārskatīšana un uzturēšana

11.1.1 [All] Privacy Lead / PIMS Manager šī politika jāpārskata reizi gadā un 30 dienu laikā pēc būtiskām izmaiņām PIMS dokumentētās informācijas prasībās.

11.1.2 [All] Privacy Lead / PIMS Manager šī politika jāpārskata 30 dienu laikā pēc būtiska audita konstatējuma, sertifikācijas neatbilstības, repozitorija platformas izmaiņām vai daudzvalodu publicēšanas procesa izmaiņām.

11.1.3 [All] Data Protection Officer / Privacy Advisor jāpārskata privātumam nozīmīgas šīs politikas izmaiņas REG12 pirms apstiprināšanas.

11.1.4 [All] Top Management jāapstiprina būtiskas šīs politikas izmaiņas REG12 pirms publicēšanas.

11.1.5 [All] Privacy Lead / PIMS Manager jāreģistrē apstiprināto šīs politikas izmaiņu paziņošana REG11 30 dienu laikā pēc publicēšanas.

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 subjekta tiesību pārvaldības politika

12.8 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.9 PII08 - Datu aizsardzības pēc projektēšanas un 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 apmācību, informētības un kompetences politika

12.18 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

13. Atsauces standarti un ietvari

13.1 Šī politika ir kartēta uz šādiem standartiem un regulējumiem. Kartējums skaidro, kā politika atbalsta citētās prasības, un identificē iekšējos punktus, ar kuriem tās tiek ieviestas vai atbalstītas.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Kartēts uz PIMS piemērojamības paziņojuma, kontroles pasākumu piemērojamības ierakstu un politiku sasaistes ar pierādījumiem uzturēšanu. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Kartēts uz dokumentētās informācijas identificēšanu, apstiprināšanu, versiju kontroli, piekļuvi, izgūšanu, saglabāšanu, atsaukšanu, tulkojuma versiju sasaisti un glabāšanas metadatiem. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Kartēts uz darbības plānošanas un kontroles pierādījumiem apstrādes ierakstiem, pierādījumu veidnēm, darbības pierādījumu kvalitāti un ārēji sniegtiem pierādījumiem. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Kartēts uz dokumentētu pierādījumu uzturēšanu par mērījumiem, izgūšanas veiktspēju, pierādījumu trūkumiem, tulkojumu neatbilstībām un repozitorija piekļuves pārskatīšanas pabeigšanu. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Kartēts uz audita pierādījumu izgūšanu, audita izlasi, audita pierādījumu izsekojamību un audita konstatējumiem, kas saistīti ar dokumentētās informācijas kontroli. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Kartēts uz vadības pārskata pierādījumiem, dokumentētās informācijas kontroles izskatīšanu vadības pārskatīšanā un Top Management pierādījumu kontroles veiktspējas pārskatīšanu. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Kartēts uz dokumentētās informācijas neatbilstībām, korektīvajām darbībām, izņēmumu pārvaldību, slēgšanu un efektivitātes verifikāciju. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Kartēts uz pārziņa apstrādes ierakstiem, pārskatatbildības ierakstiem, apstrādes pierādījumu kvalitāti un pārziņa pienākumus atbalstošo pierādījumu glabāšanu. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Kartēts uz apstrādātāja vienošanos, klienta norādījumu, ārēji sniegtiem pierādījumiem un apstrādātāja attiecību pierādījumu kontroli. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Kartēts uz PIMS ierakstu aizsardzību pret zudumu, neatļautām izmaiņām, neatļautu piekļuvi, neatļautu izpaušanu un neatbilstošu likvidēšanu. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartēts uz pārskatatbildības pierādījumiem, pierādījumu izsekojamību, pierādījumu izgūšanu, neatbilstību ierakstiem un auditam gataviem ierakstiem, kas apliecina atbilstību. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Kartēts uz pārziņa pārvaldības pierādījumiem, apstiprinājumu ierakstiem, politiku kontroli, pārskatatbildības pasākumiem, dokumentētu pārskatīšanu un Top Management pārraudzību. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Kartēts uz apstrādātāju un apakšapstrādātāju dokumentāciju, klienta norādījumu pierādījumiem, ārēji sniegtiem procesa pierādījumiem un pierādījumu izpaušanas kontroli. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Kartēts uz apstrādes ierakstu pierādījumiem, pierādījumu kvalitātes prasībām, apstrādes darbību atsaucēm un apstrādes pierādījumu īpašnieka/statusa metadatiem. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Kartēts uz pierādījumu repozitoriju aizsardzību, piekļuves ierobežojumiem, piekļuves apstiprinājumiem, repozitorija aizsardzības pārskatīšanu un neatļautas piekļuves noņemšanu. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Kartēts uz privātuma atbilstības pierādījumiem, audita pierādījumu izgūšanu, pierādījumu izsekojamību, neatkarīgas pārskatīšanas atbalstu un korektīvo darbību pierādījumiem. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Kartēts uz ar PII saistītu ierakstu aizsardzību, ierakstu saglabāšanu un pierādījumu repozitorija piekļuves un dzēšanas kontroles pasākumiem. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Kartēts uz dokumentētās informācijas identificēšanu, apstiprināšanu, pieejamību, aizsardzību, versiju kontroli, glabāšanu, galīgo apstrādi un ārēji pieprasītas dokumentētās informācijas kontroli. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Kartēts uz PIMS ierakstu aizsardzību pret zudumu, iznīcināšanu, viltošanu, neatļautu piekļuvi, neatļautu izpaušanu un neatbilstošu likvidēšanu. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Kartēts uz privātuma un PII aizsardzību dokumentētajā informācijā, pierādījumu repozitorijos, izpaušanā un piekļuves kontrolētos ierakstos. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].