					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII14					Dokumenta nosaukums: **PII drošības un piekļuves kontroles 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; Clause 8.1	Both	Primary	PII drošības kontroles pasākumu plānošana un darbība
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Pierādījumi, uzraudzība un korektīvā darbība
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitātes un piekļuves tiesības PII apstrādei
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Galiekārtu aizsardzība un droša autentifikācija
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Žurnālfiksēšana un kriptogrāfiskā aizsardzība
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Lietojumprogrammu drošība un droša arhitektūra
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Ierakstu aizsardzība un pārskatīšana
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Drošība, pārskatatbildība un apstrādātāja kontroles pasākumi
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 kontroles pasākumu integrācija
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	Norādījumi drošības kontroles pasākumu ieviešanai
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informācijas drošības un privātuma atbilstības principi
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause	Both	Supporting	PII aizsardzības drošības kontroles pasākumi

	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			

1. Piemērošanas joma

1.1 Šī politika nosaka PII specifiskās drošības un piekļuves kontroles prasības sistēmām, lietojumprogrammām, pakalpojumiem, ierīcēm, mākoņvidēm un operatīvajiem procesiem, kuros PII tiek glabāta, pārsūtīta, apstrādāta, tai piekļūst, to administrē vai aizsargā.

1.2 Šī politika attiecas uz pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja kontekstiem, kuros organizācija nosaka, ekspluatē, atbalsta vai paļaujas uz drošības kontroles pasākumiem PII apstrādei.

1.3 Šī politika aptver šādas PII drošības kontroles jomas:

1.3.1 PII drošības pamatlīmeni un integrāciju ar esošajām informācijas drošības politikām;

1.3.2 piekļuves kontroli;

1.3.3 autentifikāciju;

1.3.4 privileģēto piekļuvi;

1.3.5 šifrēšanu un drošu glabāšanu;

1.3.6 žurnālfiksēšanu un uzraudzību;

1.3.7 drošu konfigurāciju un ievainojamību pārvaldību;

1.3.8 galiekārtu un mākoņvides piekļuves kontroles pasākumus;

1.3.9 pierādījumu sasaisti ar REG02, REG08, REG10 un REG12.

1.4 Šī politika neaizstāj pilnu informācijas drošības pārvaldības sistēmu, tīkla drošības politiku, drošas izstrādes politiku, rezerves kopiju politiku, galiekārtu politiku, mākoņdrošības politiku, kriptogrāfisko standartu, ievainojamību pārvaldības procedūru vai reaģēšanas uz incidentiem procedūru. Ja šādas politikas jau pastāv, šī politika nosaka PII specifisko sasaisti un pierādījumu prasības, kas nepieciešamas PIMS apliecinājumam.

1.5 Šī politika nedublē:

1.5.1 PII apstrādes uzskaiti un tiesiskā pamata atbildību PII03;

1.5.2 privātuma risku un DPIA metodoloģiju PII07;

1.5.3 datu aizsardzības pēc projektēšanas kontrolpunktus PII08;

1.5.4 vākšanas, izmantošanas, izpaušanas un koplietošanas noteikumus PII09;

1.5.5 glabāšanas, dzēšanas un likvidēšanas izpildi PII10;

1.5.6 apstrādātāja dzīves cikla pārvaldību PII12;

1.5.7 starptautisko nosūtīšanas mehānismu kontroles pasākumus PII13;

1.5.8 incidentu un pārkāpumu darbplūsmu PII15;

1.5.9 dokumentētās informācijas pārvaldību PII17;

1.5.10 PIMS uzraudzības, audita un uzlabošanas pārvaldību PII18.

1.6 Šīs politikas izpratnē operatīvie žurnāli, drošības rīku izvades dati, piekļuves tiesību pārskatīšanas eksporti, ievainojamību pārskati un konfigurācijas pierādījumi ir pierādījumu avoti, kas tiek pievienoti kanoniskajiem pierādījumu objektiem, tajos apkopoti vai uz tiem atsaucas. Tie nav atsevišķi PIMS reģistri.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka PII visā apstrādes laikā tiek aizsargāta ar atbilstošiem, riskam samērīgiem un auditējamiem drošības un piekļuves kontroles pasākumiem.

2.2 Šī politika ļauj organizācijai pierādīt, ka PII drošības kontroles pasākumi tiek plānoti, ieviesti, pārskatīti, uzraudzīti un uzlaboti, izmantojot REG02, REG08, REG10 un REG12, neveidojot dublējošus drošības reģistrus un neaizstājot esošās informācijas drošības politikas.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 noteikt PII piekļuves kontroles pamatlīmeni sistēmām un apstrādes darbībām;

3.1.2 nodrošināt, ka autentifikācijas kontroles pasākumi ir atbilstoši PII sensitivitātei un piekļuves kontekstam;

3.1.3 noteikt prasības privileģētās un parastās piekļuves PII pārskatīšanai;

3.1.4 noteikt šifrēšanas un drošas glabāšanas prasības PII glabāšanā, pārsūtē un attiecīgajos mākoņvides vai galiekārtu kontekstos;

3.1.5 noteikt žurnālfiksēšanas un uzraudzības prasības attiecībā uz piekļuvi PII, PII izmaiņām un administrēšanu;

3.1.6 noteikt drošas konfigurācijas un ievainojamību pierādījumu prasības sistēmām, kas apstrādā PII;

3.1.7 noteikt galiekārtu un mākoņvides piekļuves prasības, neveidojot pilnu galiekārtu vai mākoņdrošības politiku;

3.1.8 sasaistīt iespējamos PII drošības incidentus ar REG10, nedublējot incidentu darbplūsmu;

3.1.9 integrēties ar esošajām informācijas drošības politikām, ja tādas ir pieejamas;

3.1.10 uzturēt auditam gatavus pierādījumus, izmantojot tikai REG02, REG08, REG10 un REG12.

4. Politikas prasības

4.1 PII drošības pamatlīmenis un ISMS integrācija

4.1.1 [Both] Information Security Lead ir jānosaka PII drošības pamatlīmenis katrai sistēmai vai pakalpojumam, kas apstrādā PII, REG12 pirms sistēmas vai pakalpojuma nodošanas ražošanas vidē vai būtiskām izmaiņām.

4.1.2 [Both] System Owner / Application Owner ir jāreģistrē ieviesto PII drošības kontroles pasākumu pierādījumu atrašanās vieta REG12, pirms PIMS apliecinājumam paļaujas uz esošu informācijas drošības kontroles pasākumu.

4.1.3 [Controller] Process Owner / Business Owner ir jāidentificē PII sensitivitāte, apstrādes konteksts un piekļuves vajadzība REG02 pirms jaunas vai būtiski mainītas piekļuves PII pieprasīšanas.

4.1.4 [Processor] Vendor / Procurement Owner ir jāreģistrē klienta drošības norādījumi, klienta atbildības robežas un apstrādātāja drošības saistības REG08 pirms apstrādātāja piekļuve klienta PII sākas vai būtiski mainās.

4.1.5 [Both] Privacy Lead / PIMS Manager ir jāpārbauda, ka PII drošības pierādījumi ir sasaistīti ar REG02, REG08, REG10 vai REG12, pirms apstrādes darbība tiek pieņemta kā PIMS auditējama.

4.2 Piekļuves kontroles pamatlīmenis

4.2.1 [Both] System Owner / Application Owner ir jāierobežo piekļuve PII līdz apstiprinātām lomām un autorizētiem lietotājiem, kas reģistrēti vai izsekojami REG02 vai REG12, pirms piekļuve tiek iespējota.

4.2.2 [Both] Process Owner / Business Owner ir jāapstiprina PII piekļuves biznesa nolūks REG02 vai REG12, pirms System Owner / Application Owner piešķir piekļuvi.

4.2.3 [Both] System Owner / Application Owner ir jāpārskata lietotāju piekļuve sistēmām, kas apstrādā augstas ietekmes vai sensitīvu PII, vismaz reizi ceturksnī un pārskatīšanas rezultāts jāreģistrē REG12.

4.2.4 [Both] System Owner / Application Owner ir jāpārskata lietotāju piekļuve citām sistēmām, kas apstrādā PII, vismaz reizi gadā un pārskatīšanas rezultāts jāreģistrē REG12.

4.2.5 [Both] System Owner / Application Owner ir jānoņem vai jāgroza PII piekļuve REG12 vienas darba dienas laikā pēc lomas maiņas, darba attiecību izbeigšanas, līguma izpildes pabeigšanas vai brīža, kad piekļuve vairs nav nepieciešama.

4.2.6 [Processor] Vendor / Procurement Owner ir jāapstiprina REG08, ka apstrādātāja piekļuve klienta PII ir ierobežota līdz dokumentētiem klienta norādījumiem, pirms piekļuve tiek iespējota vai mainīta.

4.2.7 [Subprocessor] Vendor / Procurement Owner ir jāapstiprina REG08, ka apakšapstrādātāja piekļuve PII ir ierobežota līdz autorizētām apakšapstrādes darbībām, pirms apakšapstrādātāja piekļuve tiek iespējota vai mainīta.

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

9. Izņēmumi

9.1.1 [Both] Information Security Lead ir jāreģistrē katrs izņēmums no PII drošības vai piekļuves kontroles prasības REG12 pirms izņēmuma aktivizēšanas.

9.1.2 [Both] Data Protection Officer / Privacy Advisor ir jākonsultē par augstāka riska PII drošības izņēmumiem REG12 pirms apstiprināšanas.

9.1.3 [Both] Top Management ir jāapstiprina PII drošības izņēmumi REG12 pirms aktivizēšanas, ja izņēmums ietekmē augstas ietekmes PII, sensitīvu PII, privileģēto piekļuvi, šifrēšanu, žurnālfiksēšanu vai neatrisinātas augsta riska ievainojamības.

9.1.4 [Both] Information Security Lead ir jānosaka izņēmuma beigu termiņš, kompensējošais kontroles pasākums un pārskatīšanas datums REG12 pirms izņēmuma apstiprināšanas.

9.1.5 [Both] System Owner / Application Owner ir jānovērš, jāatjauno vai jāslēdz beigušies PII drošības izņēmumi REG12 piecu darba dienu laikā pēc termiņa beigām.

9.1.6 [Processor] Vendor / Procurement Owner ir jāreģistrē apstrādātāja vai apakšapstrādātāja drošības izņēmumi, kas ietekmē klienta PII, REG08 un REG12 pirms pieņemšanas.

10. Politikas piemērošana

10.1.1 [Both] Privacy Lead / PIMS Manager ir jāreģistrē neatbilstības par trūkstošiem vai nepilnīgiem PII drošības pierādījumiem REG12 piecu darba dienu laikā pēc identificēšanas.

10.1.2 [Both] Information Security Lead ir jāpiešķir novēršanas atbildība par PII drošības kontroles pasākumu kļūmēm REG12 piecu darba dienu laikā pēc validācijas.

10.1.3 [Both] System Owner / Application Owner ir jāatspējo vai jāierobežo nesankcionēta, pārmērīga vai nepamatota PII piekļuve vienas darba dienas laikā pēc validācijas un darbība jāreģistrē REG12.

10.1.4 [Conditional] Incident Response Coordinator ir jāsasaista politikas piemērošanas darbības ar REG10 vienas darba dienas laikā, ja piemērošanas jautājums ietver iespējamu vai apstiprinātu PII incidentu.

10.1.5 [Both] Top Management ir jāpārskata atkārtotas vai augsta riska PII drošības neatbilstības REG12 pirms vadības pārskatīšanas.

11. Pārskatīšana un uzturēšana

11.1.1 [All] Privacy Lead / PIMS Manager ir jāpārskata šī politika kopā ar Information Security Lead vismaz reizi gadā un pārskatīšanas rezultāts jāreģistrē REG12.

11.1.2 [Both] Information Security Lead ir jāpārskata PII drošības pamatlīmenis REG12 30 dienu laikā pēc būtiskām tehnoloģiju, apdraudējumu, audita, incidenta vai regulatīvām izmaiņām, kas ietekmē PII drošību.

11.1.3 [Both] System Owner / Application Owner ir jāatjaunina sistēmas līmeņa PII drošības pierādījumi REG12 30 dienu laikā pēc būtiskām arhitektūras, piekļuves, konfigurācijas, ievainojamību vai žurnālfiksēšanas izmaiņām.

11.1.4 [Processor] Vendor / Procurement Owner ir jāpārskata apstrādātāja un apakšapstrādātāja PII drošības atbildību pierādījumi REG08 30 dienu laikā pēc būtiskām pakalpojuma, klienta norādījumu vai apakšapstrādātāja izmaiņām.

11.1.5 [All] Internal Audit / Compliance Reviewer ir jāpārbauda politikas pārskatīšanas pierādījumi un atlasīti PII drošības kontroles pasākumu pierādījumi REG12 saskaņā ar apstiprināto audita plānu.

12. Saistītās politikas

12.1 Šī politika jālasa kopā ar:

12.1.1 PII01 - Privātuma informācijas pārvaldības sistēmas politika;

12.1.2 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika;

12.1.3 PII03 - PII apstrādes uzskaites un tiesiskā pamata politika;

12.1.4 PII07 - Privātuma risku izvērtēšanas un DPIA politika;

12.1.5 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika;

12.1.6 PII09 - PII vākšanas, izmantošanas, izpaušanas un koplietošanas politika;

12.1.7 PII10 - PII glabāšanas, dzēšanas un likvidēšanas politika;

12.1.8 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika;

12.1.9 PII13 - Starptautiskas PII nosūtīšanas politika;

12.1.10 PII15 - PII incidentu un pārkāpumu pārvaldības politika;

12.1.11 PII16 - Privātuma apmācības, informētības un kompetences politika;

12.1.12 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika;

12.1.13 PII18 - PIMS uzraudzības, audita un uzlabošanas politika.

13. Atsauces standarti un ietvari

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].