					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: PII14					Dokumento pavadinimas: **PII saugumo ir prieigos kontrolės politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Nuostata / kontrolės priemonė / straipsnis	Taikomumas	Aprėpties tipas	Komentaras
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	PII saugumo kontrolės priemonių planavimas ir veikimas
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Įrodymai, stebėsena ir korekciniai veiksmai
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Tapatybės ir prieigos teisės PII tvarkymui
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Galinių įrenginių apsauga ir saugus autentifikavimas
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Žurnalų vedimas ir kriptografinė apsauga
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Taikomųjų programų saugumas ir saugi architektūra
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Įrašų apsauga ir peržiūra
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Saugumas, atskaitomybė ir duomenų tvarkytojų kontrolės priemonės
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 kontrolės priemonių integracija
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	Saugumo kontrolės priemonių įgyvendinimo gairės
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijos saugumo ir

				privatumo atitikties principai
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	Both	Supporting	PII apsaugos saugumo kontrolės priemonės

1. Taikymo sritis

1.1 Šioje politikoje nustatomi PII specifiniai saugumo ir prieigos kontrolės reikalavimai sistemoms, taikomosioms programoms, paslaugoms, įrenginiams, debesijos aplinkoms ir operaciniams procesams, kuriuose PII saugoma, perduodama, tvarkoma, pasiekiama, administruojama arba apsaugoma.

1.2 Ši politika taikoma duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo kontekstams, kai organizacija nustato, eksploatuoja, palaiko arba remiasi PII tvarkymo saugumo kontrolės priemonėmis.

1.3 Ši politika apima šias PII saugumo kontrolės sritis:

1.3.1 PII bazinius saugumo reikalavimus ir integraciją su esamomis informacijos saugumo politikomis;

1.3.2 prieigos kontrolę;

1.3.3 autentifikavimą;

1.3.4 privilegijuotą prieigą;

1.3.5 šifravimą ir saugų saugojimą;

1.3.6 žurnalų vedimą ir stebėseną;

1.3.7 saugų konfigūravimą ir pažeidžiamumų valdymą;

1.3.8 galinių įrenginių ir debesijos prieigos kontrolės priemones;

1.3.9 įrodymų sąsają per REG02, REG08, REG10 ir REG12.

1.4 Ši politika nepakeičia visos informacijos saugumo valdymo sistemos, tinklo saugumo politikos, saugaus kūrimo politikos, atsarginių kopijų politikos, galinių įrenginių politikos, debesijos saugumo politikos, kriptografinio standarto, pažeidžiamumų valdymo procedūros ar reagavimo į incidentus procedūros. Kai tokios politikos jau yra, ši politika nustato PII specifines sąsajas ir įrodymų reikalavimus, reikalingus PIMS patikinimui.

1.5 Ši politika nedubliuoja:

1.5.1 PII tvarkymo veiklos apskaitos ir teisinio pagrindo savininkystės pagal PII03;

1.5.2 privatumo rizikos ir DPIA metodikos pagal PII07;

1.5.3 privatumo pagal projektavimą kontrolės vartų pagal PII08;

1.5.4 rinkimo, naudojimo, atskleidimo ir dalijimosi taisyklių pagal PII09;

1.5.5 saugojimo, ištrynimo ir sunaikinimo vykdymo pagal PII10;

1.5.6 duomenų tvarkytojų gyvavimo ciklo valdysenos pagal PII12;

1.5.7 tarptautinio perdavimo priemonių kontrolės pagal PII13;

1.5.8 incidentų ir pažeidimų darbo eigos pagal PII15;

1.5.9 dokumentuotos informacijos valdysenos pagal PII17;

1.5.10 PIMS stebėsenos, audito ir tobulinimo valdysenos pagal PII18.

1.6 Šios politikos tikslais operaciniai žurnalai, saugumo priemonių išvestys, prieigos peržiūrų eksportai, pažeidžiamumų ataskaitos ir konfigūracijos įrodymai yra įrodymų šaltiniai, kurie pridedami prie kanoninių įrodymų objektų, apibendrinami juose arba nurodomi per juos. Jie nėra atskiri PIMS registrai.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad PII viso tvarkymo metu būtų apsaugoma tinkamomis, su rizika suderintomis ir audituojamomis saugumo bei prieigos kontrolės priemonėmis.

2.2 Ši politika leidžia organizacijai įrodyti, kad PII saugumo kontrolės priemonės yra planuojamos, įgyvendinamos, peržiūrimos, stebimos ir tobulinamos per REG02, REG08, REG10 ir REG12, nekuriant dubliuojančių saugumo registrų ir nepakeičiant esamų informacijos saugumo politikų.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 apibrėžti PII prieigos kontrolės bazinį lygį sistemoms ir tvarkymo veikloms;

3.1.2 užtikrinti, kad autentifikavimo kontrolės priemonės atitiktų PII jautrumą ir prieigos kontekstą;

3.1.3 nustatyti privilegijuotos ir įprastos prieigos prie PII peržiūros reikalavimus;

3.1.4 nustatyti PII šifravimo ir saugaus saugojimo lūkesčius saugomiems duomenims, perduodamiems duomenims ir atitinkamuose debesijos ar galinių įrenginių kontekstuose;

3.1.5 nustatyti žurnalų vedimo ir stebėsenos lūkesčius dėl prieigos prie PII, PII pakeitimų ir administravimo;

3.1.6 nustatyti saugaus konfigūravimo ir pažeidžiamumų įrodymų reikalavimus sistemoms, kuriose tvarkoma PII;

3.1.7 nustatyti galinių įrenginių ir debesijos prieigos lūkesčius nekuriant visos galinių įrenginių ar debesijos saugumo politikos;

3.1.8 susieti įtariamus PII saugumo incidentus su REG10, nedubliuojant incidentų darbo eigos;

3.1.9 integruoti šią politiką su esamomis informacijos saugumo politikomis, kai jos yra;

3.1.10 palaikyti auditui tinkamus įrodymus naudojant tik REG02, REG08, REG10 ir REG12.

4. Politikos nuostatos

4.1 PII baziniai saugumo reikalavimai ir ISMS integracija

4.1.1 [Both] Information Security Lead privalo REG12 apibrėžti PII bazinius saugumo reikalavimus kiekvienai sistemai ar paslaugai, kurioje tvarkoma PII, prieš sistemai ar paslaugai pradedant veikti produkcinėje aplinkoje arba prieš esminį pakeitimą.

4.1.2 [Both] System Owner / Application Owner privalo REG12 įrašyti įgyvendintos PII saugumo kontrolės priemonės įrodymų vietą prieš remdamasis esama informacijos saugumo kontrolės priemone PIMS patikinimui.

4.1.3 [Controller] Process Owner / Business Owner privalo REG02 nustatyti PII jautrumą, tvarkymo kontekstą ir prieigos poreikį prieš prašydamas naujos arba iš esmės pakeistos prieigos prie PII.

4.1.4 [Processor] Vendor / Procurement Owner privalo REG08 įrašyti kliento saugumo nurodymus, kliento atsakomybės ribas ir duomenų tvarkytojo saugumo įsipareigojimus prieš pradedant duomenų tvarkytojo prieigą prie kliento PII arba prieš ją iš esmės pakeičiant.

4.1.5 [Both] Privacy Lead / PIMS Manager privalo patikrinti, ar PII saugumo įrodymai yra susieti su REG02, REG08, REG10 arba REG12, prieš pripažindamas tvarkymo veiklą audituojama pagal PIMS.

4.2 Prieigos kontrolės bazinis lygis

4.2.1 [Both] System Owner / Application Owner privalo apriboti prieigą prie PII tik patvirtintiems vaidmenims ir autorizuotiems naudotojams, įrašytiems arba atsekamiems REG02 ar REG12, prieš įgalindamas prieigą.

4.2.2 [Both] Process Owner / Business Owner privalo REG02 arba REG12 patvirtinti PII prieigos verslo tikslą prieš System Owner / Application Owner suteikiant prieigą.

4.2.3 [Both] System Owner / Application Owner privalo ne rečiau kaip kas ketvirtį peržiūrėti naudotojų prieigą prie sistemų, kuriose tvarkoma didelio poveikio arba jautri PII, ir peržiūros rezultatą įrašyti REG12.

4.2.4 [Both] System Owner / Application Owner privalo ne rečiau kaip kartą per metus peržiūrėti naudotojų prieigą prie kitų sistemų, kuriose tvarkoma PII, ir peržiūros rezultatą įrašyti REG12.

4.2.5 [Both] System Owner / Application Owner privalo REG12 pašalinti arba pakeisti PII prieigą per vieną darbo dieną po vaidmens pasikeitimo, darbo santykių nutraukimo, sutarties užbaigimo arba kai prieiga nebėra reikalinga.

4.2.6 [Processor] Vendor / Procurement Owner privalo REG08 patvirtinti, kad duomenų tvarkytojo prieiga prie kliento PII yra apribota dokumentuotais kliento nurodymais, prieš įgalinant arba pakeičiant prieigą.

4.2.7 [Subprocessor] Vendor / Procurement Owner privalo REG08 patvirtinti, kad subtvarkytojo prieiga prie PII yra apribota autorizuotomis subtvarkymo veiklomis, prieš įgalinant arba pakeičiant subtvarkytojo prieigą.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Išimtys

9.1.1 [Both] Information Security Lead privalo REG12 įrašyti kiekvieną PII saugumo arba prieigos kontrolės reikalavimo išimtį prieš ją aktyvuojant.

9.1.2 [Both] Data Protection Officer / Privacy Advisor privalo konsultuoti dėl didesnės rizikos PII saugumo išimčių REG12 prieš patvirtinimą.

9.1.3 [Both] Top Management privalo REG12 patvirtinti PII saugumo išimtis prieš aktyvavimą, kai išimtis daro poveikį didelio poveikio PII, jautriai PII, privilegijuotai prieigai, šifravimui, žurnalų vedimui arba neišspręstiems didelės rizikos pažeidžiamumams.

9.1.4 [Both] Information Security Lead privalo REG12 apibrėžti išimties galiojimo pabaigą, kompensuojančią kontrolės priemonę ir peržiūros datą prieš išimties patvirtinimą.

9.1.5 [Both] System Owner / Application Owner privalo REG12 pašalinti, atnaujinti arba uždaryti pasibaigusio galiojimo PII saugumo išimtis per penkias darbo dienas po galiojimo pabaigos.

9.1.6 [Processor] Vendor / Procurement Owner privalo REG08 ir REG12 įrašyti duomenų tvarkytojo arba subtvarkytojo saugumo išimtis, darančias poveikį kliento PII, prieš priėmimą.

10. Įgyvendinimo užtikrinimas

10.1.1 [Both] Privacy Lead / PIMS Manager privalo REG12 įrašyti neatitiktis dėl trūkstamų arba neišsamių PII saugumo įrodymų per penkias darbo dienas nuo nustatymo.

10.1.2 [Both] Information Security Lead privalo REG12 priskirti PII saugumo kontrolės priemonių nesuveikimų šalinimo savininkystę per penkias darbo dienas nuo patvirtinimo.

10.1.3 [Both] System Owner / Application Owner privalo per vieną darbo dieną nuo patvirtinimo išjungti arba apriboti neautorizuotą, perteklinę arba nepagrįstą PII prieigą ir veiksmą įrašyti REG12.

10.1.4 [Conditional] Incident Response Coordinator privalo per vieną darbo dieną susieti įgyvendinimo užtikrinimo veiksmus su REG10, kai įgyvendinimo užtikrinimo klausimas yra susijęs su įtariamu arba patvirtintu PII incidentu.

10.1.5 [Both] Top Management privalo REG12 peržiūrėti pasikartojančias arba didelės rizikos PII saugumo neatitiktis prieš vadovybės peržiūrą.

11. Peržiūra ir priežiūra

11.1.1 [All] Privacy Lead / PIMS Manager privalo ne rečiau kaip kartą per metus kartu su Information Security Lead peržiūrėti šią politiką ir peržiūros rezultatą įrašyti REG12.

11.1.2 [Both] Information Security Lead privalo REG12 peržiūrėti PII bazinius saugumo reikalavimus per 30 dienų po esminio technologijų, grėsmių, audito, incidento arba reglamentavimo pokyčio, darančio poveikį PII saugumui.

11.1.3 [Both] System Owner / Application Owner privalo REG12 atnaujinti sistemos lygmens PII saugumo įrodymus per 30 dienų po esminio architektūros, prieigos, konfigūracijos, pažeidžiamumų arba žurnalų vedimo pakeitimo.

11.1.4 [Processor] Vendor / Procurement Owner privalo REG08 peržiūrėti duomenų tvarkytojo ir subtvarkytojo PII saugumo atsakomybės įrodymus per 30 dienų po esminio paslaugos, kliento nurodymų arba subtvarkytojo pakeitimo.

11.1.5 [All] Internal Audit / Compliance Reviewer privalo pagal patvirtintą audito planą patikrinti politikos peržiūros įrodymus ir atrinktus PII saugumo kontrolės priemonių įrodymus REG12.

12. Susijusios politikos

12.1 Ši politika turėtų būti skaitoma kartu su:

12.2 PII01 - Privatumo informacijos valdymo sistemos politika;

12.3 PII02 - Privatumo vaidmenų, atsakomybių ir atskaitomybės politika;

12.4 PII03 - PII tvarkymo veiklos apskaitos ir teisinio pagrindo politika;

12.5 PII07 - Privatumo rizikos vertinimo ir DPIA politika;

12.6 PII08 - Privatumo pagal projektavimą ir pagal numatytuosius nustatymus politika;

12.7 PII09 - PII rinkimo, naudojimo, atskleidimo ir dalijimosi politika;

12.8 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika;

12.9 PII12 - Duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių privatumo valdymo politika;

12.10 PII13 - Tarptautinio PII perdavimo politika;

12.11 PII15 - PII incidentų ir pažeidimų valdymo politika;

12.12 PII16 - Privatumo mokymo, informuotumo ir kompetencijos politika;

12.13 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika;

12.14 PII18 - PIMS stebėsenos, audito ir tobulinimo politika.

13. Pamatiniai standartai ir sistemos

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].