					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: PII17					Dokumento pavadinimas: **PIMS dokumentuotos informacijos ir įrodymų valdymo 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	Punktas / kontrolės priemonė / straipsnis	Taikomumas	Aprėpties tipas	Komentaras
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA dokumentuota informacija
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS dokumentuota informacija
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operacinių įrodymų kontrolė
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Stebėsenos įrodymai
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Audito įrodymai
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Vadovybės peržiūros įrodymai
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neatitikties ir korekcinių veiksmų įrodymai
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Duomenų valdytojo tvarkymo įrašai
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Duomenų tvarkytojo susitarimo ir nurodymų įrodymai
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Įrašų apsauga
GDPR	Article 5(2)	Controller	Supporting	Atskaitomybės įrodymai
GDPR	Article 24	Controller	Supporting	Duomenų valdytojo priemonės ir įrodymai
GDPR	Article 28	Both	Supporting	Duomenų tvarkytojo dokumentacija
GDPR	Article 30	Both	Supporting	Tvarkymo įrašai
GDPR	Article 32	Both	Supporting	Įrodymų apsauga
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privatumo atitikties įrodymai
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Įrašų apsauga

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Dokumentuotos informacijos kontrolė
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Įrašų apsauga
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Privatumo ir PII apsauga

1. Taikymo sritis

1.1 Ši politika nustato privalomus PIMS dokumentuotos informacijos kūrimo, tvirtinimo, versijavimo, apsaugos, saugojimo, gavimo, vertimo, atšaukimo ir pagrindimo įrodymais reikalavimus.

1.2 Ši politika taikoma PIMS politikoms, registrams, dokumentuotiems patvirtinimams, įrodymų įrašams, audito įrodymams, vadovybės peržiūros įrašams, korekcinių veiksmų įrodymams ir kontroliuojamiems vertimams, naudojamiems PIMS atitikčiai įrodyti.

1.3 Ši politika taikoma duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo kontekstams.

1.4 Ši politika nesukuria atskiro dokumentų kontrolės registro. Dokumentuotos informacijos kontrolės įrodymai tvarkomi naudojant kanoninius PIMS įrodymų objektus nuo REG01 iki REG12, o REG03 ir REG12 naudojami kontrolės priemonių taikomumui, auditui, neatitikčiai, korekciniams veiksmams ir tobulinimo įrodymams.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad PIMS dokumentuota informacija būtų tiksli, kontroliuojama, prieinama autorizuotiems naudotojams, apsaugota nuo neteisėto pakeitimo ar atskleidimo, saugoma audituojamumui užtikrinti ir atšaukiama, kai tampa nebegaliojanti.

2.2 Ši politika palaiko pasirengimą sertifikavimui užtikrindama, kad įrodymus, reikalingus PIMS atitikčiai įrodyti, būtų galima rasti, patikrinti, gauti ir susieti su taikomomis politikomis, kontrolės priemonėmis, tvarkymo veiklomis, rizikomis, auditais ir korekciniais veiksmais.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 nustatyti PIMS dokumentuotos informacijos kontrolės reikalavimus;

3.1.2 palaikyti įrodymų vientisumą nuo REG01 iki REG12;

3.1.3 užtikrinti, kad politikų ir įrodymų tvirtinimas būtų atsekamas;

3.1.4 užtikrinti, kad versijų istorija ir atšaukimo sprendimai būtų dokumentuoti;

3.1.5 susieti PIMS įrodymus su Taikomumo pareiškimu ir politikų susiejimais;

3.1.6 kontroliuoti prieigą prie PIMS dokumentų ir įrodymų įrašų;

3.1.7 palaikyti daugiakalbių politikų ir įrodymų versijų kontrolę;

3.1.8 sudaryti galimybę laiku gauti audito įrodymus;

3.1.9 užkirsti kelią nereikalingai dokumentų kontrolės biurokratijai;

3.1.10 išsaugoti auditui tinkamus įrašus sertifikavimui, klientų patikinimui ir nuolatiniam tobulinimui.

4. Politikos nuostatos

4.1 PIMS dokumentuotos informacijos kontrolė

4.1.1 [All] Privacy Lead / PIMS Manager privalo palaikyti PIMS dokumentuotos informacijos indeksą REG12 prieš pirminį PIMS paskelbimą ir vėliau kas ketvirtį.

4.1.2 [All] Process Owner / Business Owner privalo REG02 nustatyti dokumentuotą informaciją, reikalingą kiekvienai jam priklausančiai PII tvarkymo veiklai, prieš pradedant tvarkymo veiklą ir vėliau kasmet.

4.1.3 [All] Privacy Lead / PIMS Manager privalo susieti taikomas PIMS politikas, kontrolės priemones ir įrodymų pareigas su REG03 prieš kiekvieną politikos išleidimą ir per 15 darbo dienų nuo bet kokio esminio kontrolės priemonių taikomumo pakeitimo.

4.1.4 [All] Privacy Lead / PIMS Manager privalo kiekvienai PIMS dokumentuotos informacijos kategorijai REG12 priskirti prieigos lygį ir įrodymų jautrumo klasifikaciją prieš pradedant naudoti kategoriją.

4.2 Kūrimas, tvirtinimas, versijavimas ir paskelbimas

4.2.1 [All] Privacy Lead / PIMS Manager privalo REG12 priskirti dokumento identifikatorių, savininką, versijos numerį, patvirtinimo būseną, įsigaliojimo datą ir peržiūros datą prieš paskelbiant PIMS dokumentuotą informaciją.

4.2.2 [All] Top Management privalo REG12 patvirtinti pagrindines PIMS politikas ir esminius politikų pakeitimus prieš jų paskelbimą.

4.2.3 [All] Privacy Lead / PIMS Manager privalo REG12 patvirtinti PIMS įrodymų šablonus arba įterptąsias registro skiltis prieš operacinį naudojimą.

4.2.4 [All] Privacy Lead / PIMS Manager privalo REG12 įrašyti versijų istoriją ir pakeitimo pagrindimą prieš išleidžiant atnaujintą PIMS dokumentuotą informaciją.

4.2.5 [All] Privacy Lead / PIMS Manager privalo REG11 įrašyti komunikaciją apie patvirtintus PIMS dokumentuotos informacijos pakeitimus per 30 dienų nuo paskelbimo.

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

9. Išimtys

9.1.1 [All] Process Owner / Business Owner privalo REG12 paprašyti dokumentuotos informacijos arba įrodymų kontrolės išimčių prieš nukrypdamas nuo šios politikos.

9.1.2 [All] Privacy Lead / PIMS Manager privalo REG12 įvertinti kiekvieną dokumentuotos informacijos arba įrodymų kontrolės išimtį per 10 darbo dienų nuo prašymo.

9.1.3 [All] Data Protection Officer / Privacy Advisor privalo REG12 įrašyti konsultaciją prieš patvirtinant bet kokią išimtį, susijusią su PII įrodymų atskleidimu, vertimo neatitikimu, saugojimo konfliktu ar audito įrodymų apribojimu.

9.1.4 [All] Top Management privalo REG12 patvirtinti dokumentuotos informacijos išimtis, viršijančias 30 dienų arba darančias poveikį sertifikavimui, didelės rizikos tvarkymui ar išoriniam patikinimui, prieš išimčiai įsigaliojant.

9.1.5 [All] Privacy Lead / PIMS Manager privalo REG12 nustatyti kiekvienos patvirtintos dokumentuotos informacijos arba įrodymų kontrolės išimties galiojimo pabaigos datą, neviršijančią 90 dienų.

9.1.6 [All] Privacy Lead / PIMS Manager privalo REG12 uždaryti arba pakartotinai įvertinti kiekvieną dokumentuotos informacijos arba įrodymų kontrolės išimtį per penkias darbo dienas nuo galiojimo pabaigos.

10. Įgyvendinimo užtikrinimas

10.1.1 [All] Privacy Lead / PIMS Manager privalo REG12 įrašyti trūkstamą, netikslią, nekontroliuojamą, pasenusią ar negaunamą PIMS dokumentuotą informaciją kaip neatitiktį per penkias darbo dienas nuo nustatymo.

10.1.2 [All] Privacy Lead / PIMS Manager privalo neleisti paskelbti PIMS dokumentuotos informacijos, kai REG12 trūksta privalomo patvirtinimo, versijos, savininko ar įsigaliojimo datos įrodymų.

10.1.3 [All] Process Owner / Business Owner privalo neleisti audito tikslais teikti tvarkymo įrodymų, kai REG02 trūksta privalomų savininko, datos, būsenos ar patvirtinimo įrodymų.

10.1.4 [All] System Owner / Application Owner privalo pašalinti neautorizuotą prieigą prie PIMS dokumentuotos informacijos saugyklų ir REG12 įrašyti pašalinimą per vieną darbo dieną nuo nustatymo.

10.1.5 [All] Internal Audit / Compliance Reviewer privalo REG12 patikrinti korekcinių veiksmų veiksmingumą dokumentuotos informacijos neatitiktims per kitą suplanuotą auditą arba per 60 dienų nuo uždarymo, atsižvelgiant į tai, kas įvyksta anksčiau.

11. Peržiūra ir priežiūra

11.1.1 [All] Privacy Lead / PIMS Manager privalo peržiūrėti šią politiką kasmet ir per 30 dienų nuo esminio PIMS dokumentuotos informacijos reikalavimų pakeitimo.

11.1.2 [All] Privacy Lead / PIMS Manager privalo peržiūrėti šią politiką per 30 dienų po reikšmingos audito išvados, sertifikavimo neatitikties, saugyklos platformos pakeitimo ar daugiakalbio paskelbimo proceso pakeitimo.

11.1.3 [All] Data Protection Officer / Privacy Advisor privalo REG12 peržiūrėti privatumo požiūriu reikšmingus šios politikos pakeitimus prieš patvirtinimą.

11.1.4 [All] Top Management privalo REG12 patvirtinti esminius šios politikos pakeitimus prieš paskelbimą.

11.1.5 [All] Privacy Lead / PIMS Manager privalo REG11 įrašyti komunikaciją apie patvirtintus šios politikos pakeitimus per 30 dienų nuo paskelbimo.

12. Susijusios politikos

12.1 Šią politiką palaiko šios susijusios politikos:

12.2 PII01 - Privačios informacijos apsaugos valdymo sistemos politika

12.3 PII02 - Privatumo vaidmenų, atsakomybių ir atskaitomybės politika

12.4 PII03 - PII tvarkymo apskaitos ir teisinio pagrindo politika

12.5 PII04 - Privatumo pranešimo ir skaidrumo politika

12.6 PII05 - Sutikimų ir nuostatų valdymo politika

12.7 PII06 - Duomenų subjektų teisių valdymo politika

12.8 PII07 - Privatumo rizikos vertinimo ir DPIA politika

12.9 PII08 - Privatumo pagal projektavimą ir pagal numatytuosius nustatymus politika

12.10 PII09 - PII rinkimo, naudojimo, atskleidimo ir dalijimosi politika

12.11 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika

12.12 PII11 - PII tikslumo ir kokybės politika

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

12.14 PII13 - Tarptautinio PII perdavimo politika

12.15 PII14 - PII saugumo ir prieigos kontrolės politika

12.16 PII15 - PII incidentų ir pažeidimų valdymo politika

12.17 PII16 - Privatumo mokymų, informuotumo ir kompetencijos politika

12.18 PII18 - PIMS stebėsenos, audito ir tobulinimo politika

13. Pamatiniai standartai ir sistemos

13.1 Ši politika susieta su toliau nurodytais standartais ir reglamentais. Susiejimas paaiškina, kaip politika palaiko nurodytus reikalavimus, ir identifikuoja vidinius punktus, kuriais jie įgyvendinami arba palaikomi.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Susieta su PIMS taikomumo pareiškimo, kontrolės priemonių taikomumo įrašų ir politikų bei įrodymų sąsajų palaikymu. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Susieta su dokumentuotos informacijos identifikavimu, tvirtinimu, versijų kontrole, prieiga, gavimu, išsaugojimu, atšaukimu, vertimo versijų sąsaja ir saugojimo metaduomenimis. 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** - Susieta su operacinio planavimo ir kontrolės įrodymais tvarkymo įrašams, įrodymų šablonais, operacinių įrodymų kokybe ir iš išorės pateiktais įrodymais. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Susieta su dokumentuotų matavimo, gavimo veiksmingumo, įrodymų spragų, vertimo neatitikimų ir saugyklų prieigos peržiūros užbaigimo įrodymų palaikymu. 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** - Susieta su audito įrodymų gavimu, audito atranka, audito įrodymų atsekamumu ir audito išvadomis, susijusiomis su dokumentuotos informacijos kontrole. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Susieta su vadovybės peržiūros įrodymais, vadovybės peržiūros metu nagrinėjama dokumentuotos informacijos kontrole ir Top Management atliekama įrodymų kontrolės veiksmingumo peržiūra. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Susieta su dokumentuotos informacijos neatitiktimis, korekciniais veiksmais, išimčių tvarkymu, uždarymu ir veiksmingumo patikrinimu. 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** - Susieta su duomenų valdytojo tvarkymo įrašais, atskaitomybės įrašais, tvarkymo įrodymų kokybe ir įrodymų, pagrindžiančių duomenų valdytojo pareigas, saugojimu. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Susieta su duomenų tvarkytojo susitarimu, kliento nurodymu, iš išorės pateiktais įrodymais ir santykių su duomenų tvarkytoju įrodymų kontrole. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Susieta su PIMS įrašų apsauga nuo praradimo, neteisėto pakeitimo, neteisėtos prieigos, neteisėto atskleidimo ir netinkamo sunaikinimo. 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)** - Susieta su atskaitomybės įrodymais, įrodymų atsekamumu, įrodymų gavimu, neatitikčių įrašais ir auditui tinkamais įrašais, įrodančiais atitiktį. 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** - Susieta su duomenų valdytojo valdysenos įrodymais, patvirtinimo įrašais, politikų kontrole, atskaitomybės priemonėmis, dokumentuota peržiūra ir Top Management priežiūra. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Susieta su duomenų tvarkytojo ir subtvarkytojo dokumentacija, kliento nurodymų įrodymais, iš išorės pateiktais proceso įrodymais ir įrodymų atskleidimo kontrole. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Susieta su tvarkymo įrašų įrodymais, įrodymų kokybės reikalavimais, tvarkymo veiklos nuorodomis ir tvarkymo įrodymų savininko bei būsenos metaduomenimis. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Susieta su įrodymų saugyklų apsauga, prieigos apribojimais, prieigos patvirtinimais, saugyklų apsaugos peržiūra ir neautorizuotos prieigos pašalinimu. 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** - Susieta su privatumo atitikties įrodymais, audito įrodymų gavimu, įrodymų atsekamumu, nepriklausomos peržiūros palaikymu ir korekcinių veiksmų įrodymais. 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** - Susieta su PII susijusių įrašų apsauga, įrašų išsaugojimu ir įrodymų saugyklų prieigos bei ištrynimo kontrolės priemonėmis. 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** - Susieta su dokumentuotos informacijos identifikavimu, tvirtinimu, prieinamumu, apsauga, versijų kontrole, saugojimu, galutiniu sutvarkymu ir išorės reikalaujamos dokumentuotos informacijos kontrole. 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 - Susieta su PIMS įrašų apsauga nuo praradimo, sunaikinimo, klastojimo, neteisėtos prieigos, neteisėto atskleidimo ir netinkamo sunaikinimo. 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 - Susieta su privatumo ir PII apsauga dokumentuotoje informacijoje, įrodymų saugyklose, atskleidimuose ir prieigos kontroliuojamuose įrašuose. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].