					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: PII16					Dokumento pavadinimas: **Privatumo mokymų, informuotumo ir kompetencijos 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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Kompetencija ir informuotumas
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacija ir dokumentuoti įrodymai
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operacinė kontrolė, matavimas ir tobulinimas
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Informuotumas apie PII tvarkymą, švietimas ir mokymai
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Atskaitomybė, duomenų tvarkytojo valdysena, saugumas ir DPO užduotys
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetencija, informuotumas ir mokymai
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Informuotumo, švietimo ir mokymų gairės
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijos saugumo ir privatumo atitiktis

1. Taikymo sritis

1.1 Ši politika nustato organizacijos reikalavimus privatumo mokymams, informuotumui ir kompetencijai privačios informacijos apsaugos valdymo sistemoje.

1.2 Ši politika taikoma personalui, rangovams, laikinam personalui, atitinkamoms trečiosioms šalims, duomenų tvarkytojams, subtvarkytojams ir kitoms suinteresuotosioms šalims, kurių darbas gali turėti įtakos PII tvarkymui, PIMS veiksmingumui, duomenų subjektų teisėms, privatumo rizikai, su PII susijusiam informacijos saugumui, duomenų tvarkytojo nurodymams, privatumo incidentams, dokumentuotai informacijai arba atitikties įrodymams.

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

1.4 Ši politika apima:

1.4.1 privatumo mokymų auditorijos identifikavimą;

1.4.2 įvadinius mokymus;

1.4.3 metinius pakartotinius mokymus;

1.4.4 vaidmenimis pagrįstus ir įvykių inicijuojamus mokymus;

1.4.5 mokymų baigimo įrodymus;

1.4.6 mokymų nebaigimo eskalavimą;

1.4.7 mokymų efektyvumo peržiūrą;

1.4.8 duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių mokymų patikinimo įrodymus.

1.5 Ši politika nesukuria atskiros mokymų matricos, mokymų valdymo skydo, žmogiškųjų išteklių registro, kompetencijų registro, drausminių priemonių registro ar klientų mokymų registro.

1.6 Mokymų priskyrimai, užbaigimai, priminimai, kompetencijos įrodymai ir informuotumo įrodymai registruojami REG11, o išimtys, eskalavimai, neatitiktys, korekciniai veiksmai ir peržiūros įrodymai registruojami REG12.

1.7 Duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių mokymų patikinimo įrodymai, kai aktualu, registruojami REG08.

1.8 Ši politika nedubliuoja:

1.8.1 vaidmenų atskaitomybės priskyrimo PII02;

1.8.2 tvarkymo veiklos apskaitos ir teisinio pagrindo reikalavimų PII03;

1.8.3 privatumo rizikos ir DPIA metodikos PII07;

1.8.4 privatumo pagal projektavimą kontrolės vartų PII08;

1.8.5 duomenų tvarkytojo gyvavimo ciklo valdysenos PII12;

1.8.6 PII saugumo ir prieigos kontrolės vykdymo PII14;

1.8.7 PII incidentų ir pažeidimų darbo eigos PII15;

1.8.8 dokumentuotos informacijos valdysenos PII17;

1.8.9 stebėsenos, vidaus audito ir tobulinimo valdysenos PII18.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad asmenys, kurių darbas turi įtakos PII tvarkymui, suprastų savo privatumo atsakomybes, nustatytu periodiškumu baigtų tinkamus mokymus, išlaikytų su vaidmeniu susijusią kompetenciją ir sukurtų audituojamus mokymų, informuotumo ir eskalavimo įrodymus.

2.2 Ši politika palaiko nuoseklų PIMS įgyvendinimą, naudojant REG11 kaip pagrindinį mokymų ir informuotumo įrodymų objektą, o REG08, REG10 ir REG12 – kaip pagalbinius įrodymų objektus.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 apibrėžti privatumo mokymų auditorijas;

3.1.2 apibrėžti įvadinių mokymų reikalavimus;

3.1.3 apibrėžti metinių pakartotinių mokymų reikalavimus;

3.1.4 apibrėžti vaidmenimis pagrįstų privatumo mokymų reikalavimus;

3.1.5 registruoti baigimo įrodymus REG11;

3.1.6 eskaluoti mokymų nebaigimo atvejus per REG12;

3.1.7 kai aktualu, REG08 palaikyti duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių mokymų patikinimo įrodymus;

3.1.8 peržiūrėti mokymų efektyvumą nekuriant perteklinių rodiklių ar dubliuojančių registrų;

3.1.9 užtikrinti, kad mokymų turinys išliktų suderintas su galiojančiomis PIMS politikomis ir esminiais privatumo įsipareigojimais.

4. Politikos nuostatos

4.1 Mokymų auditorija ir priskyrimas

4.1.1 [All] Privacy Lead / PIMS Manager privalo apibrėžti PIMS mokymų auditorijos kategorijas REG11 prieš prasidedant kiekvienam metiniam mokymų ciklui.

4.1.2 [All] Process Owner / Business Owner privalo REG11 identifikuoti personalą, kurio pareigos apima PII tvarkymą, prieš įvedimą į darbą, vaidmens priskyrimą ar esminį pareigų pasikeitimą.

4.1.3 [Conditional] System Owner / Application Owner privalo REG11 identifikuoti naudotojus, kuriems reikalingi PII sistemos, privilegijuotos prieigos ar administraciniai privatumo mokymai, prieš suteikiant prieigą arba ją iš esmės pakeičiant.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager privalo REG11 arba REG08 užregistruoti bendrų duomenų valdytojų mokymų atsakomybės paskirstymą prieš prasidedant bendrai tvarkymo veiklai arba jai iš esmės pasikeičiant.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor privalo REG11 identifikuoti išplėstinių privatumo mokymų poreikius prieš priskiriant mokymus vaidmenims, kurie vykdo didelės rizikos tvarkymą, specialių kategorijų PII, duomenų subjektų teisių įgyvendinimą, DPIAs, tarptautinius perdavimus arba pažeidimų vertinimą.

4.1.6 [All] Privacy Lead / PIMS Manager privalo REG11 užregistruoti priskirtą mokymų auditoriją, mokymų tipą, privalomą baigimo datą ir įrodymų savininką prieš prasidedant kiekvienam metiniam mokymų ciklui.

4.2 Įvadinių ir metinių mokymų periodiškumas

4.2.1 [All] Privacy Lead / PIMS Manager privalo REG11 priskirti bazinius privatumo informuotumo mokymus per 10 darbo dienų nuo įdarbinimo pradžios personalui, turinčiam prieigą prie PII arba PIMS atsakomybių.

4.2.2 [All] Process Owner / Business Owner privalo užtikrinti, kad priskirtas personalas REG11 baigtų įvadinius privatumo mokymus prieš patvirtinant neprižiūrimą prieigą prie PII arba per 30 dienų nuo įdarbinimo pradžios, atsižvelgiant į tai, kas įvyksta anksčiau.

4.2.3 [All] Privacy Lead / PIMS Manager privalo REG11 priskirti metinius privatumo žinių atnaujinimo mokymus bent kartą per 12 mėnesių.

4.2.4 [All] Process Owner / Business Owner privalo REG11 patvirtinti priskirto personalo metinių pakartotinių mokymų baigimo būseną iki paskelbtos metinės termino datos.

4.2.5 [Conditional] Privacy Lead / PIMS Manager privalo REG11 priskirti tikslinius pakartotinius mokymus per 30 dienų po esminio privatumo politikos pakeitimo, esminio PIMS proceso

pakeitimo, audito išvados, pasikartojančios mokymų nesėkmės arba aktualios PII incidento pamokos.

[... 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 užregistruoti privatumo mokymų išimties prašymą prieš pratęsiant privalomą baigimo terminą.

9.1.2 [All] Privacy Lead / PIMS Manager privalo REG12 patvirtinti arba atmesti privatumo mokymų išimties prašymus prieš išimčiai įsigaliojant.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor privalo REG12 konsultuoti dėl mokymų išimčių prieš patvirtinimą, kai išimtis daro įtaką didelės rizikos tvarkymui, specialių kategorijų PII, teisių nagrinėjimui, incidentų tvarkymui, tarptautiniams perdavimams arba sertifikavimo įrodymams.

9.1.4 [Conditional] Top Management privalo REG12 patvirtinti privatumo mokymų išimtis prieš aktyvavimą, kai išimtis daro įtaką pasikartojančiam mokymų nebaigimui, privilegijuotai prieigai prie PII, didelio poveikio PII tvarkymui arba reguliuotojams teikiamiems įrodymams.

9.1.5 [All] Privacy Lead / PIMS Manager privalo REG12 apibrėžti išimties savininką, galiojimo pabaigos datą, kompensuojantį veiksmą ir peržiūros datą prieš patvirtindamas bet kurią privatumo mokymų išimtį.

9.1.6 [All] Process Owner / Business Owner privalo REG12 uždaryti arba atnaujinti patvirtintas privatumo mokymų išimtis iki išimties galiojimo pabaigos datos.

10. Įgyvendinimo užtikrinimas

10.1.1 [All] Privacy Lead / PIMS Manager privalo REG12 užregistruoti mokymų neatitiktį per penkias darbo dienas, kai privalomų privatumo mokymų įrodymai yra trūkstami, neišsamūs, vėluojami arba neužtikrinamas jų atsekamumas iki REG11.

10.1.2 [All] Process Owner / Business Owner privalo užtikrinti, kad vėluojami privalomieji privatumo mokymai būtų baigti arba eskaluoti REG11 arba REG12 per 10 darbo dienų po vėlavimo būsenos užregistravimo.

10.1.3 [Conditional] System Owner / Application Owner privalo REG12 apriboti naują didelio poveikio PII prieigą, kai privalomi įvadiniai arba vaidmenimis pagrįsti privatumo mokymai po eskalavimo išlieka nebaigti.

10.1.4 [Processor] Vendor / Procurement Owner privalo REG08 ir REG12 eskaluoti trūkstamus duomenų tvarkytojo, subtvarkytojo arba išorinės darbo jėgos mokymų patikinimo įrodymus per penkias darbo dienas po identifikavimo.

10.1.5 [Conditional] Incident Response Coordinator privalo su REG10 susieti su mokymais susijusius įgyvendinimo užtikrinimo veiksmus per vieną darbo dieną, kai mokymų nesėkmė prisidėjo prie įtariamo arba patvirtinto PII incidento.

10.1.6 [All] Internal Audit / Compliance Reviewer privalo patikrinti REG12 mokymų korekcinių veiksmų užbaigimo įrodymus per kitą suplanuotą auditą arba per 60 dienų nuo užbaigimo, atsižvelgiant į tai, kas įvyksta anksčiau.

11. Peržiūra ir palaikymas

11.1.1 [All] Privacy Lead / PIMS Manager privalo bent kartą per metus peržiūrėti šią politiką ir mokymų turinį bei REG11 arba REG12 užregistruoti peržiūros rezultatą.

11.1.2 [All] Privacy Lead / PIMS Manager privalo peržiūrėti šią politiką per 30 dienų po esminio PIMS taikymo srities, privatumo teisės aktų, tvarkymo veiklos, vaidmenų modelio, incidentų pamokų, audito išvadų arba mokymų efektyvumo rezultatų pakeitimo.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor privalo REG12 peržiūrėti privatumo požiūriu reikšmingus 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 atnaujinti REG11 mokymų turinį ir priskyrimo įrodymus per 30 dienų po patvirtinto esminio politikos pakeitimo.

12. Susijusios politikos

12.1 Ši politika turėtų būti skaitoma kartu su:

12.2 PII01 - Privačios informacijos apsaugos 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 PII04 - Privatumo pranešimų 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 PII12 - Duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių privatumo valdymo politika;

12.13 PII13 - Tarptautinio PII perdavimo politika;

12.14 PII14 - PII saugumo ir prieigos kontrolės politika;

12.15 PII15 - PII incidentų ir pažeidimų valdymo politika;

12.16 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika;

12.17 PII18 - PIMS stebėsenos, audito ir tobulinimo politika.

13. Pamatiniai standartai ir sistemos

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].