					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: PII18					Dokumento pavadinimas: **PIMS stebėsenos, audito ir tobulinimo 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 6.2	Both	Supporting	Privatumo tikslų matavimas
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Stebėsenos, audito ir tobulinimo dokumentuota informacija
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operacinio planavimo ir kontrolės stebėsena
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Stebėsena, matavimas, analizė ir vertinimas
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Vidaus auditas
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Vadovybės peržiūra
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Nuolatinis tobulinimas
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neatitiktis ir korekcinis veiksmas
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Duomenų valdytojo tvarkymo įrašai, naudojami auditui
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Duomenų tvarkytojo susitarimo ir bendradarbiavimo audito metu įrodymai
GDPR	Article 5(2)	Controller	Supporting	Atskaitomybės įrodymai
GDPR	Article 24	Controller	Supporting	Duomenų valdytojo priemonės ir veiksmingumo peržiūra
GDPR	Article 28	Both	Supporting	Duomenų tvarkytojo audito ir bendradarbiavimo valdysena

GDPR	Article 30	Both	Supporting	Tvarkymo įrašai, naudojami auditui
GDPR	Article 32	Both	Supporting	Saugumo priemonių testavimas ir vertinimas
GDPR	Article 39	Conditional	Supporting	DPO stebėsena ir konsultacijos audito klausimais, kai taikoma
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Privatumo atitiktis, auditas ir nepriklausoma priežiūra
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	PII apsaugos peržiūra ir atitikties patikros
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Informacijos saugumo stebėsena ir vertinimas
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS vidaus audito palaikymas
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS vadovybės peržiūros palaikymas
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS nuolatinio tobulinimo palaikymas
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS neatitikčių ir korekcinių veiksmų palaikymas
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Nepriklausoma informacijos saugumo peržiūra
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Politikų ir standartų atitikties peržiūra
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Valdymo sistemos audito principai, programa, atlikimas ir kompetencija

1. Taikymo sritis

1.1 Šioje politikoje nustatomi organizacijos reikalavimai PIMS stebėsenai, matavimui, analizei, vertinimui, vidaus auditui, vadovybės peržiūrai, neatitikčių tvarkymui, korekciniams veiksmams ir nuolatiniam tobulinimui.

1.2 Ši politika taikoma toliau nurodytiems objektams:

1.2.1 visiems PIMS procesams, kontrolės priemonėms, politikoms, registrams, įrodymų objektams, sistemoms, tiekėjams, duomenų tvarkytojams, subtvarkytojams ir duomenų dalijimosi susitarimams, patenkantiems į PIMS taikymo sritį;

1.2.2 organizacijos duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo kontekstams;

1.2.3 konsoliduotai PIMS veiksmingumo, privatumo tikslų, kontrolės priemonių įgyvendinimo būsenos, audito išvadų, neatitikčių, korekcinių veiksmų, vadovybės peržiūros veiksmų ir tobulinimo veiksmų stebėsenai;

1.2.4 įrodymams, saugomiems REG12, ir pagalbiniams pirminiams įrodymams, saugomiems REG01–REG11.

1.3 Ši politika nepakeičia operacinės stebėsenos reikalavimų, apibrėžtų kitose PIMS politikose. Ji nustato konsoliduotą PIMS veiklos vertinimo, audito, peržiūros ir tobulinimo ciklą.

1.4 Šioje politikoje reikšminga PIMS neatitiktis reiškia pažeidimą, kuris reikšmingai paveikia PIMS taikymo sritį, privatumo tikslus, atskaitomybę už PII tvarkymą, privatumo rizikos tvarkymą, duomenų subjekto teises, tvarkymo saugumą, duomenų tvarkytojo ar subtvarkytojo valdyseną, pasirengimą pažeidimams, dokumentuotų įrodymų vientisumą, sertifikavimo taikymo sritį arba yra pakartotinis to paties reikalavimo nesilaikymas per 12 mėnesių laikotarpį.

1.5 Šioje politikoje esminis pokytis reiškia bet kokį pokytį, darantį poveikį PIMS taikymo sričiai, PII tvarkymo tikslams, PII kategorijoms, duomenų subjektų kategorijoms, tvarkymo vietoms, duomenų valdytojo ar duomenų tvarkytojo vaidmenų paskirstymui, sistemos architektūrai, tiekėjų ar subtvarkytojų susitarimams, privatumo rizikos profiliui, taikomoms teisinėms ar sutartinėms prievolėms, audito taikymo sričiai, stebėsenos metodui arba sertifikavimo taikymo sričiai.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad organizacija vertintų PIMS veiksmingumą, tikrintų PIMS atitiktį, nustatytų neatitiktis, taisytų kontrolės priemonių silpnąsias vietas ir nuolat tobulintų PIMS remdamasi objektyviais įrodymais.

2.2 Ši politika leidžia organizacijai įrodyti, kad PIMS stebėsenos, audito, vadovybės peržiūros ir tobulinimo veiklos yra suplanuotos, nepriklausomos, kai to reikalaujama, grindžiamos įrodymais, atliekamos laiku ir atsekamos iki atsakingų vaidmenų bei kanoninių įrodymų objektų.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 apibrėžti konsoliduotą PIMS stebėsenos ir matavimo procesą;

3.1.2 užtikrinti, kad privatumo tikslai ir PIMS kontrolės priemonių veiksmingumas būtų matuojami naudojant dokumentuotus įrodymus;

3.1.3 nustatyti rizika grindžiamą PIMS vidaus audito programą;

3.1.4 išsaugoti nepriklausomumą ir objektyvumą PIMS audito veiklose;

3.1.5 užtikrinti, kad vadovybės peržiūrai būtų pateikiami išsamūs ir aktualūs PIMS veiksmingumo įvesties duomenys;

3.1.6 užtikrinti, kad neatitiktys būtų registruojamos, vertinamos, ištaisomos ir patikrinamos;

3.1.7 užtikrinti, kad korekciniai veiksmai būtų sekami iki užbaigimo ir peržiūrimi dėl veiksmingumo;

3.1.8 nustatyti pasikartojančias silpnąsias vietas ir tobulinimo galimybes;

3.1.9 palaikyti pasirengimą sertifikavimui ir atskaitingą įrodymų valdymą;

3.1.10 vengti dubliuoti operacinius rodiklius, kurie jau apibrėžti susijusiose PIMS politikose.

4. Politikos nuostatos

4.1 PIMS stebėsenos ir matavimo sistema

4.1.1 [Both] Privacy Lead / PIMS Manager privalo apibrėžti konsoliduotą PIMS stebėsenos programą REG12 prieš pradinį PIMS veikimą ir kasmet po to.

4.1.2 [Both] Privacy Lead / PIMS Manager privalo apibrėžti kiekvieno PIMS rodiklio matavimo metodą, dažnį, įrodymų šaltinį, tikslinę reikšmę ir atsakingą vaidmenį REG12 prieš prasidedant matavimo ciklui.

4.1.3 [Both] Process Owner / Business Owner privalo kas ketvirtį pateikti PII tvarkymo veiklos stebėsenos įvesties duomenis iš REG02 Privacy Lead / PIMS Manager.

4.1.4 [Both] Information Security Lead privalo kas ketvirtį pateikti PII saugumo kontrolės priemonių būsenos įvesties duomenis iš REG03 Privacy Lead / PIMS Manager.

4.1.5 [Both] Vendor / Procurement Owner privalo kas ketvirtį pateikti duomenų tvarkytojų, subtvarkytojų, dalijimosi su trečiosiomis šalimis ir tiekėjų patikinimo būsenos įvesties duomenis iš REG08 Privacy Lead / PIMS Manager.

4.1.6 [All] Incident Response Coordinator privalo kas mėnesį ir per 10 darbo dienų po reikšmingo incidento užbaigimo pateikti privatumo incidentų ir pažeidimų tendencijų įvesties duomenis iš REG10 Privacy Lead / PIMS Manager.

4.1.7 [Both] Privacy Lead / PIMS Manager privalo kas ketvirtį konsoliduoti PIMS stebėsenos rezultatus REG12.

4.2 PIMS vidaus audito programa

4.2.1 [All] Internal Audit / Compliance Reviewer privalo kasmet prieš pirmąjį suplanuotą PIMS audito ciklą parengti rizika grindžiamą PIMS vidaus audito programą REG12.

4.2.2 [All] Internal Audit / Compliance Reviewer privalo prieš pradedant audito lauko darbus REG12 apibrėžti kiekvieno PIMS audito tikslą, kriterijus, taikymo sritį, metodą, imties pagrindą ir ataskaitos pateikimo terminą.

4.2.3 [All] Internal Audit / Compliance Reviewer privalo prieš kiekvieną audito paskyrimą REG12 užregistruoti auditoriaus nepriklausomumo ir interesų konflikto patikras.

4.2.4 [All] Privacy Lead / PIMS Manager privalo per REG12 per 10 darbo dienų nuo patvirtinto audito prašymo pateikti prašomą kontroliuojamą PIMS dokumentuotą informaciją ir registrų įrodymus.

4.2.5 [Both] Internal Audit / Compliance Reviewer privalo kiekvieno PIMS audito metu patikrinti taikomų PIMS kontrolės priemonių įgyvendinimo būseną pagal REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer privalo kiekvieno PIMS audito metu REG12 užregistruoti pasirinktą PII tvarkymo įrodymų imtį.

4.2.7 [All] Internal Audit / Compliance Reviewer privalo per 15 darbo dienų po audito užbaigimo užregistruoti PIMS audito rezultatus REG12.

4.2.8 [All] Privacy Lead / PIMS Manager privalo per 10 darbo dienų nuo audito rezultatų priėmimo REG12 priskirti korekcinių veiksmų savininkus priimtoms PIMS audito išvadoms.

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

9. Išimtys

9.1 Stebėsenos, audito ir tobulinimo išimtys

9.1.1 [All] Process Owner / Business Owner privalo prieš įvykstant nukrypimui REG12 paprašyti bet kokios šios politikos išimties.

9.1.2 [All] Privacy Lead / PIMS Manager privalo per 10 darbo dienų nuo prašymo REG12 įvertinti kiekvienos prašomos išimties poveikį privatumui, sertifikavimui, auditui ir korekciniams veiksmams.

9.1.3 [All] Data Protection Officer / Privacy Advisor privalo prieš patvirtinant bet kokią išimtį, darančią poveikį teisinėms prievolėms, duomenų subjekto teisėms, DPIA įsipareigojimams, kliento audito prievolėms arba didelės rizikos tvarkymui, REG12 užregistruoti konsultaciją.

9.1.4 [All] Top Management privalo prieš įsigaliojant išimčiai REG12 patvirtinti išimtis, darančias poveikį audito grafiko įvykdymui, vadovybės peržiūrai, reikšmingoms neatitiktims, sertifikavimo taikymo sričiai arba didelės rizikos tvarkymui.

9.1.5 [All] Privacy Lead / PIMS Manager privalo kiekvienai patvirtintai stebėsenos, audito arba tobulinimo išimčiai REG12 nustatyti galiojimo pabaigos datą, neviršijančią 90 dienų.

9.1.6 [All] Privacy Lead / PIMS Manager privalo per penkias darbo dienas nuo galiojimo pabaigos REG12 uždaryti arba iš naujo įvertinti kiekvieną stebėsenos, audito arba tobulinimo išimtį.

10. Vykdymo užtikrinimas

10.1 Stebėsenos, audito ir tobulinimo reikalavimų vykdymo užtikrinimas

10.1.1 [All] Privacy Lead / PIMS Manager privalo per penkias darbo dienas nuo nustatymo REG12 užregistruoti praleistą stebėsenos ciklą, praleistą PIMS auditą, vėluojančią vadovybės peržiūrą, trūkstamus audito įrodymus, vėluojantį korekcinį veiksmą arba vėluojantį tobulinimo veiksmą kaip neatitiktį.

10.1.2 [All] Internal Audit / Compliance Reviewer privalo prieš audito ataskaitos išleidimą REG12 užregistruoti audito išvados sunkumą.

10.1.3 [All] Top Management privalo per 10 darbo dienų nuo eskalavimo REG12 pareikalauti korekcinio veiksmo kiekvienai reikšmingai PIMS neatitikčiai.

10.1.4 [All] Process Owner / Business Owner privalo užkirsti kelią didelės rizikos tvarkymo paleidimui gamybinėje aplinkoje arba išorinio patikinimo pateikimui, kai reikalaujami korekcinio veiksmo įrodymai prieš paleidimą gamybinėje aplinkoje arba pateikimą nėra REG12.

10.1.5 [All] Privacy Lead / PIMS Manager privalo per penkias darbo dienas po antro pasikartojimo per 12 mėnesių laikotarpį REG12 eskaluoti pasikartojančius praleistus stebėsenos arba korekcinių veiksmų terminus Top Management.

10.1.6 [All] Internal Audit / Compliance Reviewer privalo REG12 patikrinti vykdymo užtikrinimo veiksmo uždarymą per kitą suplanuotą auditą arba per 60 dienų nuo pranešto uždarymo, atsižvelgiant į tai, kas įvyksta anksčiau.

11. Peržiūra ir priežiūra

11.1 Politikos peržiūra ir priežiūra

11.1.1 [All] Privacy Lead / PIMS Manager privalo kasmet ir per 30 dienų nuo esminio PIMS stebėsenos, audito, vadovybės peržiūros, korekcinių veiksmų arba sertifikavimo reikalavimų pokyčio REG12 peržiūrėti šią politiką.

11.1.2 [All] Internal Audit / Compliance Reviewer privalo kasmet po paskutinio suplanuoto PIMS veiklos metų audito REG12 peržiūrėti PIMS audito programos veiksmingumą.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager privalo per 15 darbo dienų po patvirtintų šios politikos pakeitimų, kurie keičia PIMS taikymo sritį arba kontrolės priemonių taikomumą, atnaujinti REG01 ir REG03.

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

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 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo 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 vidaus punktus, kurie juos įgyvendina arba palaiko.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Susieta su PIMS tikslų ir PIMS veiksmingumo rodiklių apibrėžimu, matavimu, ataskaitų teikimu ir peržiūra. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Susieta su dokumentuotos informacijos apie stebėsenos rezultatus, audito programas, audito rezultatus, vadovybės peržiūros įrodymus, neatitiktis, korekcinius veiksmus ir tobulinimo veiksmus palaikymu. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Susieta su suplanuoto PIMS stebėsenos, audito, korekcinių veiksmų ir tobulinimo ciklo vykdymu kaip PIMS operacinės kontrolės dalimi. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Susieta su nustatymu, kas stebima ir matuojama, stebėsenos rezultatų konsolidavimu, PIMS veiksmingumo vertinimu ir matavimo įrodymų palaikymu. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Susieta su vidaus audito programos palaikymu, audito planavimu, auditoriaus nepriklausomumo patikromis, įrodymų atranka, audito rezultatais ir audito išvadų tolesne priežiūra. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Susieta su vadovybės peržiūros planavimu, PIMS veiksmingumo peržiūra, audito ir korekcinių veiksmų tendencijų peržiūra, rezultatų patvirtinimu ir sprendimais dėl išteklių. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Susieta su PIMS tinkamumo, pakankamumo ir veiksmingumo nuolatinio tobulinimo galimybių nustatymu, patvirtinimu, įgyvendinimu ir sekimu. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Susieta su neatitikčių registravimu, pagrindinės priežasties analize, korekcinių veiksmų planavimu, korekcinių veiksmų įgyvendinimu, veiksmingumo patikrinimu, eskalavimu ir vykdymo užtikrinimu. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Susieta su duomenų valdytojo tvarkymo įrašais, naudojamais kaip stebėsenos, audito imčių ir tvarkymo veiklos apskaitos aktualumo rodiklių įrodymų šaltiniai. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Susieta su duomenų tvarkytojo susitarimo, kliento audito, patikinimo atsakymo ir duomenų tvarkytojo bendradarbiavimo įrodymais, sekamais per tiekėjų ir klientų patikinimo procesus. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Susieta su atskaitomybės įrodymais dėl stebėsenos, audito, vadovybės peržiūros, korekcinių veiksmų ir nuolatinio tobulinimo. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Susieta su duomenų valdytojo valdysenos priemonėmis, veiksmingumo peržiūra, vadovybės peržiūra, korekciniais veiksmais ir dokumentuotais tobulinimo įrodymais. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Susieta su duomenų tvarkytojų, subtvarkytojų, klientų audito, trečiųjų šalių patikinimo ir tiekėjų bendradarbiavimo įrodymais. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Susieta su tvarkymo įrašais, naudojamais kaip stebėsenos, audito imčių, įrodymų objektų išsamumo ir tvarkymo veiklos apskaitos aktualumo įrodymai. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Susieta su PII saugumo kontrolės priemonių būsenos stebėsena ir vertinimu, techninių kontrolės priemonių įrodymais ir su saugumu susijusiais veiksmingumo įrodymais. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Susieta su Data Protection Officer / Privacy Advisor teikiamomis privatumo konsultacijomis, stebėsenos pastabomis, audito palaikymu ir privatumo atitikties tendencijų peržiūra, kai taikoma. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Susieta su privatumo atitikties tikrinimu, vidaus arba nepriklausomais auditais, vidaus kontrolės priemonėmis, priežiūros mechanizmais ir privatumo rizikos vertinimo įrodymais. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Susieta su nepriklausoma su PII susijusio informacijos saugumo peržiūra, atitiktimi politikoms ir standartams bei technine atitikties peržiūra dėl PII apsaugos. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Susieta su informacijos saugumo stebėsenos ir vertinimo įvesties duomenimis, kurie palaiko PIMS veiksmingumo matavimą ir PII saugumo kontrolės priemonių būseną. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Susieta su ISMS vidaus audito palaikymu PIMS audito planavimui, audito įrodymams, audito rezultatams ir audito programos užbaigimui. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Susieta su vadovybės peržiūros įvesties duomenimis ir rezultatais, skirtais integruotai PIMS ir informacijos saugumo veiksmingumo priežiūrai. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Susieta su PIMS ir ją palaikančios informacijos saugumo kontrolės aplinkos nuolatiniu tobulinimu. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Susieta su neatitikčių tvarkymu, korekcinių veiksmų planavimu, korekcinių veiksmų įgyvendinimu ir veiksmingumo patikrinimu. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Susieta su nepriklausoma peržiūra, auditoriaus nepriklausomumo patikromis, audito įrodymų testavimu ir nepriklausomu korekcinių veiksmų veiksmingumo patikrinimu. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Susieta su PIMS ir informacijos saugumo politikų atitikties peržiūra, kontrolės priemonių įgyvendinimo būsena ir atitikties standartams įrodymais. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Susieta su audito principais, audito programos valdymu, audito atlikimu, įrodymais grindžiamu audito ataskaitų teikimu, audito tolesne priežiūra ir auditoriaus kompetencijos lūkesčiais PIMS auditams. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].