					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: PII15-FS					Dokumento pavadinimas: **Finansų sektoriaus PII incidentų ir pažeidimų 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	Nuostata / kontrolė / straipsnis	Taikymas	Aprėpties tipas	Komentaras
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS komunikacija ir dokumentuoti incidentų įrodymai
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operacinė kontrolė, privatumo rizikos vertinimas ir sąsaja su rizikos tvarkymu
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Stebėsena, vertinimas, neatitiktis, korekciniai veiksmai ir tobulinimas
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidentų valdymo planavimas ir pasirengimas PII tvarkymui
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reagavimas į informacijos saugumo incidentus, susijusius su PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Teisiniai, įstatyminiai, reglamentavimo ir sutartiniai reikalavimai bei įrašų apsauga
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Duomenų tvarkytojo kliento susitarimas ir pagalba vykdant kliento pareigas
GDPR	Article 5(2); Article 24	Controller	Supporting	Atskaitomybė ir duomenų valdytojo atsakomybė
GDPR	Article 26	Joint Controller	Supporting	Bendrų duomenų valdytojų atsakomybės už incidentus koordinavimas
GDPR	Article 28	Both	Supporting	Duomenų tvarkytojo pagalba

				ir sutartinės duomenų tvarkytojo pareigos
GDPR	Article 32	Both	Supporting	Tvarkymo saugumas ir pažeidimų aptikimo galimybės
GDPR	Article 33	Both	Primary	Pranešimas apie asmens duomenų saugumo pažeidimą ir pažeidimo dokumentavimas
GDPR	Article 34	Controller	Primary	Informavimas apie asmens duomenų saugumo pažeidimus paveiktiems duomenų subjektams
GDPR	Article 39	Conditional	Supporting	DPO konsultacijos, stebėsena, bendradarbiavimas ir kontaktinio punkto palaikymas
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Su IRT susijusių incidentų valdymo procesas į taikymo sritį patenkantiems finansų subjektams
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Su IRT susijusių incidentų ir reikšmingų kibernetinių grėsmių klasifikavimo kriterijai
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Pranešimai apie didelius su IRT susijusius incidentus ir pranešimai apie reikšmingas kibernetines grėsmes
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Ataskaitų turinys, terminai, šablonai ir procedūros

NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Pranešimas apie reikšmingus incidentus, kai taikoma
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informacijos saugumo ir privatumo atitikties principai
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Atsakomybės reaguojant į PII incidentus ir pranešimas apie įvykius
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentų planavimas, vertinimas, reagavimas, įgyta patirtis ir įrodymų rinkimas
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incidentų valdymo proceso gyvavimo ciklas
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentų politika, planas, informuotumas, testavimas ir įgyta patirtis
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Aptikimo, pranešimo, pirminio įvertinimo, analizės, reagavimo ir ataskaitų teikimo operacijos
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Viešosios debesijos duomenų tvarkytojo pranešimo ir pažeidimo įrašų lūkesčiai

1. Taikymo sritis

1.1 Ši politika nustato reikalavimus, kaip finansų sektoriaus PIMS taikymo srityse identifikuoti, pranešti, atlikti pirminį įvertinimą, klasifikuoti, vertinti, lokalizuoti, teikti pranešimus, dokumentuoti, uždaryti ir tobulinti veiksmus, susijusius su PII incidentais ir PII pažeidimais.

1.2 **Įgyvendinimo pastaba:** ši politika yra finansų sektoriui skirta PII15 pakeičianti versija. Ji negali būti įgyvendinama kartu su PII15 tai pačiai PIMS taikymo sričiai, verslo padaliniui, produktui, kliento aplinkai, reglamentuojamai paslaugai ar įrodymų ribai. Organizacijos turi pasirinkti arba PII15, arba PII15-FS tai pačiai taikymo sričiai, kad būtų išvengta dubliuojamų incidentų valdymo pareigų, dubliuojamų registrų ir dubliuojamo audito įrodymų darbo.

1.3 Ši politika taikoma:

1.3.1 organizacijai, veikiančiai kaip PII duomenų valdytojas finansų sektoriaus kontekste;

1.3.2 organizacijai, veikiančiai kaip bendras duomenų valdytojas, kai reikia koordinuoti atsakomybę už incidentą ar pažeidimą;

1.3.3 organizacijai, veikiančiai kaip PII duomenų tvarkytojas finansų sektoriaus klientams;

1.3.4 organizacijai, veikiančiai kaip subtvarkytojas finansų sektoriaus klientams arba aukštesnės grandies duomenų tvarkytojams;

1.3.5 sistemoms, taikomosioms programoms, paslaugoms, procesams, tiekėjams, duomenų tvarkytojams, subtvarkytojams ir trečiosioms šalims, kurie tvarko, saugo, perduoda, palaiko, pasiekia ar kitaip daro poveikį PII finansų sektoriaus PIMS taikymo srityje.

1.4 Ši politika naudoja REG10 - PII incidentų ir pažeidimų registrą kaip pagrindinį finansų sektoriaus PII incidentų ir pažeidimų valdymo įrodymų objektą.

1.5 Ši politika naudoja pagalbinius įrodymų objektus taip:

1.5.1 REG01 - PIMS taikymo sričiai, taikomam suinteresuotųjų šalių, sektoriaus, kliento, sutartiniam ir pranešimų teikimo kontekstui.

1.5.2 REG02 - paveiktoms tvarkymo veikloms, PII kategorijoms, duomenų subjektų kategorijoms, tikslams, sistemoms ir paslaugoms.

1.5.3 REG03 - Taikomumo pareiškimui ir kontrolės taikymo atnaujinimams, įskaitant PII15 pakeitimą PII15-FS tai pačiai taikymo sričiai.

1.5.4 REG04 - privatumo rizikai, DPIA, liekamajai rizikai ir rizikos tvarkymo sąsajai.

1.5.5 REG08 - duomenų tvarkytojų, subtvarkytojų, klientų, tiekėjų ir trečiųjų šalių incidentų sąsajos įrodymams.

1.5.6 REG09 - tarptautinio perdavimo sąsajai, kai incidentas paveikia tarpvalstybinį tvarkymą.

1.5.7 REG11 - mokymų, informuotumo ir reagavimo į incidentus kompetencijos įrodymams.

1.5.8 REG12 - audito, neatitikties, korekcinių veiksmų, vadovybės peržiūros ir tobulinimo įrodymams.

1.6 Ši politika remiasi susijusiomis PIMS politikomis dėl specializuotų kontrolės priemonių:

1.6.1 PII03 reglamentuoja tvarkymo veiklos apskaitą ir teisinio pagrindo įrašus.

1.6.2 PII04 reglamentuoja privatumo pranešimo ir skaidrumo kontrolės priemones, nesusijusias su konkrečia komunikacija dėl pažeidimo.

1.6.3 PII06 reglamentuoja prašymus įgyvendinti duomenų subjektų teises, kylančius prieš incidentą, jo metu arba po jo.

1.6.4 PII07 reglamentuoja privatumo rizikos vertinimo ir DPIA metodiką.

1.6.5 PII08 reglamentuoja privatumo pagal projektavimą ir privatumo pagal numatytuosius nustatymus kontrolės priemones.

1.6.6 PII10 reglamentuoja saugojimo, ištrynimo ir sunaikinimo kontrolės priemones.

1.6.7 PII12 reglamentuoja duomenų tvarkytojų, subtvarkytojų, tiekėjų ir trečiųjų šalių privatumo santykių kontrolės priemones.

1.6.8 PII13 reglamentuoja tarptautinio PII perdavimo priemones ir perdavimo rizikos įrašus.

1.6.9 PII14 reglamentuoja prevencines ir nustatomąsias PII saugumo ir prieigos kontrolės priemones.

1.6.10 PII16 reglamentuoja privatumo mokymus, informuotumą ir kompetenciją.

1.6.11 PII17 reglamentuoja dokumentuotos informacijos ir įrodymų valdymą.

1.6.12 PII18 reglamentuoja stebėseną, vidaus auditą, vadovybės peržiūrą, neatitiktis, korekcinius veiksmus ir nuolatinį tobulinimą.

1.6.13 PII23 reglamentuoja debesijos PII duomenų tvarkytojo kontrolės priemones, kai debesijos duomenų tvarkytojo pareigos patenka į taikymo sritį.

1.7 Šioje politikoje:

1.7.1 „PII incidentas“ reiškia įtariamą arba patvirtintą įvykį, kuris paveikė, galėjo paveikti arba pagrįstai galėtų paveikti PII konfidencialumą, vientisumą, prieinamumą, teisėtą tvarkymą ar autorizuotą tvarkymą.

1.7.2 „PII pažeidimas“ reiškia patvirtintą PII incidentą, susijusį su neautorizuotu, neteisėtu, atsitiktiniu ar netyčiniu PII sunaikinimu, praradimu, pakeitimu, atskleidimu, prieiga prie PII, neprieinamumu ar kompromitavimu.

1.7.3 „Finansų sektoriaus PII incidentas“ reiškia PII incidentą, kuris paveikia, gali paveikti arba yra pagrįstai susijęs su reglamentuojamomis finansinėmis paslaugomis, finansų sektoriaus klientais, finansinėmis sandorio šalimis, finansinėmis operacijomis, finansų sektoriaus veikla arba finansų sektoriaus PII tvarkymu.

1.7.4 „Reikšmingas finansų sektoriaus incidentas“ reiškia finansų sektoriaus PII incidentą arba susijusį IRT incidentą, kuris atitinka REG10 dokumentuotus reikšmingumo arba pranešimo kriterijus.

1.7.5 „Reikšminga kibernetinė grėsmė“ reiškia REG10 užregistruotą kibernetinę grėsmę, kuri galėtų reikšmingai paveikti į taikymo sritį patenkančias finansų sektoriaus paslaugas, PII tvarkymą, klientus, sandorio šalis ar operacijas.

1.7.6 „Pažeidimo vertinimas“ reiškia dokumentuotą vertinimą, ar PII incidentas yra PII pažeidimas, kokia PII ir kurie duomenų subjektai paveikti, kokios rizikos gali kilti, kokie pranešimai ar komunikacija reikalingi ir kokių taisomųjų veiksmų reikia.

1.7.7 „Sužinojimas“ reiškia momentą, kai organizacija turi pagrįstą tikrumo laipsnį, kad įvyko saugumo arba privatumo incidentas ir PII buvo arba galėjo būti kompromituota.

1.7.8 „Didelio poveikio finansų sektoriaus PII incidentas“ reiškia PII incidentą, susijusį su didelės rizikos tvarkymu, specialių kategorijų arba itin jautria PII, didelio masto PII, pažeidžiamais asmenimis, reglamentuojamais klientais, reikšmingu paslaugos sutrikimu, finansinėmis sandorio šalimis, finansinėmis operacijomis, kelių jurisdikcijų poveikiu, privilegijuotos prieigos kompromitavimu, viešu atskleidimu, išpirkos reikalaujančia programine įranga, paslaugos neprieinamumu arba reikšmingu operaciniu, klientų, finansiniu ar reputaciniu poveikiu.

1.7.9 „Esminis incidento pokytis“ reiškia naują arba pasikeitusią informaciją, turinčią įtakos incidento apimčiai, sunkumui, PII kategorijoms, poveikiui duomenų subjektams, poveikiui paslaugai, finansų sektoriaus klasifikacijai, pranešimo sprendimui, poveikiui klientui, pagrindinei priežasčiai, lokalizavimui, atkūrimui, korekciniam veiksmui arba išorės ataskaitų teikimo pareigoms.

2. Tikslas

2.1 Šios politikos tikslas – užtikrinti, kad finansų sektoriaus kontekstuose PII incidentai ir pažeidimai būtų valdomi nuosekliai, laiku, teisėtai, saugiai ir su auditui tinkamais įrodymais.

2.2 Ši politika palaiko atskaitomybę reikalaudama finansų sektoriaus PII incidentus ir pažeidimus registruoti REG10 ir susieti su paveiktais tvarkymo įrašais, privatumo rizikomis, duomenų tvarkytojų ir subtvarkytojų santykiais, perdavimo įrašais, korekciniais veiksmais, mokymų įrašais, finansų sektoriaus ataskaitų teikimo sprendimais ir vadovybės peržiūros įrodymais, kai tai inicijuojama.

2.3 Ši politika užtikrina, kad duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo pareigos būtų tvarkomos pagal atskiras taikymo taisykles, kartu išlaikant vieną integruotą finansų sektoriaus incidentų ir pažeidimų įrodymų modelį.

3. Tikslai

3.1 Šios politikos tikslai yra:

3.1.1 užtikrinti, kad įtariami finansų sektoriaus PII incidentai būtų pranešami ir registruojami laiku;

3.1.2 užtikrinti, kad finansų sektoriaus PII incidentams būtų atliekamas pirminis įvertinimas ir jie būtų klasifikuojami pagal nuoseklius privatumo, saugumo, operacinius ir sektoriaus kriterijus;

3.1.3 užtikrinti, kad pažeidimo vertinimuose būtų atsižvelgiama į paveiktą PII, duomenų subjektus, sistemas, paslaugas, tvarkymo veiklas, duomenų tvarkytojus, subtvarkytojus, perdavimus, rizikas, klientus, sandorio šalis ir taisomuosius veiksmus;

3.1.4 užtikrinti, kad duomenų valdytojo pranešimo ir komunikacijos duomenų subjektams sprendimai būtų dokumentuojami;

3.1.5 užtikrinti, kad duomenų tvarkytojo ir subtvarkytojo pranešimai apie pažeidimus klientams arba aukštesnės grandies šalims būtų teikiami be nepagrįsto delsimo ir pagal taikomus susitarimus;

3.1.6 užtikrinti, kad finansų sektoriaus ataskaitų teikimo inicijavimo pagrindai būtų įvertinti, dokumentuoti ir stebimi, kai taikoma;

3.1.7 užtikrinti, kad incidento valdymo metu įrodymai būtų išsaugoti ir apsaugoti;

3.1.8 užtikrinti, kad lokalizavimas, pašalinimas, atkūrimas ir patvirtinimas būtų sekami per REG10;

3.1.9 užtikrinti, kad reikšmingos kibernetinės grėsmės ir reikšmingi finansų sektoriaus incidentai būtų nukreipiami į atitinkamas sprendimų priėmimo ir ataskaitų teikimo darbo eigas;

3.1.10 užtikrinti, kad įgyta incidentų patirtis lemtų korekcinius veiksmus, mokymus, kontrolės priemonių tobulinimą ir vadovybės peržiūrą;

3.1.11 užtikrinti, kad incidentų ir pažeidimų įrašai būtų prieinami auditui, vadovybės peržiūrai, klientų patikinimui ir reglamentavimo institucijų peržiūrai, kai taikoma;

3.1.12 užtikrinti, kad PII15-FS pakeistų PII15 tai pačiai finansų sektoriaus taikymo sričiai ir nedubliuotų PII15 įrodymų darbo.

4. Politikos nuostatos

4.1 Versijos aktyvavimas, pasirengimas ir registravimas

4.1.1 [Conditional] Privacy Lead / PIMS Manager privalo dokumentuoti PII15-FS aktyvavimą REG01 ir REG03 prieš naudojant šią politiką finansų sektoriaus PIMS taikymo sričiai.

4.1.2 [Conditional] Privacy Lead / PIMS Manager privalo REG03 ir REG12 dokumentuoti, kad PII15 nėra įgyvendinama kartu tai pačiai finansų sektoriaus PIMS taikymo sričiai, prieš patvirtinant PII15-FS.

4.1.3 [All] Incident Response Coordinator privalo kiekvieną praneštą ar aptiktą įtariamą finansų sektoriaus PII incidentą užregistruoti REG10 per vieną darbo dieną nuo gavimo arba anksčiau, kai gali būti inicijuotas taikomas pranešimo, kliento ar ataskaitų teikimo terminas.

4.1.4 [Conditional] Privacy Lead / PIMS Manager privalo palaikyti finansų sektoriaus PII incidentų ir pažeidimų valdymo kriterijus REG10 bent kartą per metus ir po bet kokio esminio PIMS taikymo srities, teisinio konteksto, klientų pareigų, sutartinių pareigų, sektoriaus ataskaitų teikimo konteksto ar didelės rizikos tvarkymo pokyčio.

4.1.5 [Both] Information Security Lead privalo per 24 valandas po to, kai įtariamas incidentas paveikia sistemą, paslaugą ar taikomąją programą, tvarkančią PII, REG10 patvirtinti incidento įrodymų išsaugojimo reikalavimus.

4.1.6 [Conditional] Vendor / Procurement Owner privalo prieš įtraukiant į veiklą ir bent kartą per metus į taikymo sritį patenkantiems duomenų tvarkytojams, subtvarkytojams, tiekėjams ir išoriniams ataskaitų teikimo paslaugų teikėjams REG08 palaikyti finansų sektoriaus trečiųjų šalių incidentų kontaktinius duomenis ir įrodymų nukreipimo reikalavimus.

4.2 Klasifikavimas ir pažeidimo vertinimas

4.2.1 [All] Incident Response Coordinator privalo per 24 valandas nuo registravimo kiekvieną REG10 įrašą suklasifikuoti kaip ne PII įvykį, įtariamą PII incidentą, patvirtintą PII incidentą, patvirtintą PII pažeidimą, finansų sektoriaus PII incidentą, reikšmingą finansų sektoriaus incidentą, reikšmingą kibernetinę grėsmę arba klasifikavimo laukiantį įrašą.

4.2.2 [Conditional] Information Security Lead privalo REG10 įvertinti paveiktas paslaugas, klientus, sandorio šalis, operacijas, paslaugos prastovą, geografinį paplitimą, duomenų praradimą, paslaugos kritiškumą ir ekonominį poveikį, kai PII incidentas gali paveikti finansų sektoriaus paslaugas ar operacijas.

4.2.3 [Both] Privacy Lead / PIMS Manager privalo nustatyti paveiktą tvarkymo veiklą, PII kategorijas, duomenų subjektų kategorijas, sistemas, duomenų tvarkytojus, subtvarkytojus, perdavimo vietas ir privatumo rizikas REG02, REG04, REG08, REG09 ir REG10 prieš galutinai priimant sprendimą dėl pranešimo apie pažeidimą.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor privalo įvertinti riziką paveiktiems duomenų subjektams dėl kiekvieno patvirtinto arba pagrįstai įtariamo PII pažeidimo ir REG10 įrašyti pranešimo rekomendaciją, rizikos pagrindimą ir konsultaciją prieš priimant išorinio pranešimo sprendimą.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager privalo per 24 valandas po bendros atsakomybės už įtariamą ar patvirtintą PII pažeidimą nustatymo REG08 ir REG10 įrašyti bendrų duomenų valdytojų atsakomybės už incidentą paskirstymą.

4.2.6 [Processor] Privacy Lead / PIMS Manager privalo per 24 valandas po to, kai įtariamas ar patvirtintas PII pažeidimas paveikia tvarkymą, atliekamą kaip duomenų tvarkytojo, REG08 ir REG10 įvertinti kliento nurodymus, sutartines pranešimo pareigas ir bendradarbiavimo pareigas.

4.2.7 [Subprocessor] Vendor / Procurement Owner privalo per 24 valandas po to, kai įtariamas ar patvirtintas PII incidentas paveikia tvarkymą, atliekamą kaip subtvarkytojo, REG08 ir REG10 nustatyti aukštesnės grandies pranešimų seką ir reikiamą įrodymų nukreipimą.

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

9. Išimtys

9.1.1 [All] Privacy Lead / PIMS Manager privalo REG12 įrašyti bet kokią šios politikos išimtį prieš ją įgyvendinant arba per 24 valandas po skubaus veiksmo, kai išankstinis patvirtinimas nebuvo įmanomas.

9.1.2 [Conditional] Top Management privalo prieš incidento uždarymą patvirtinti bet kokią išimtį, kuri reikšmingai paveikia pranešimo apie pažeidimą terminą, finansų sektoriaus ataskaitų teikimo terminą, viešąją komunikaciją, įsipareigojimą klientui, įrodymų išsaugojimą arba riziką duomenų subjektui, o patvirtinimo įrodymai turi būti saugomi REG10 ir REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor privalo prieš incidento uždarymą dokumentuoti konsultaciją dėl bet kokio pavėluoto pranešimo, nepranešimo sprendimo, ataskaitų teikimo išimties arba išimtinio komunikacijos būdo, o konsultacija turi būti saugoma REG10.

9.1.4 [Both] Vendor / Procurement Owner privalo per penkias darbo dienas po išimties nustatymo REG08 ir REG12 įrašyti tiekėjo, duomenų tvarkytojo, subtvarkytojo, kliento arba išorinio paslaugų teikėjo išimtis, darančias poveikį finansų sektoriaus reagavimui į incidentus.

9.1.5 [All] Privacy Lead / PIMS Manager privalo bent kartą per mėnesį iki uždarymo peržiūrėti atviras šios politikos išimtis, o peržiūros būsena turi būti saugoma REG12.

10. Politikos laikymosi užtikrinimas

10.1.1 [All] Process Owner / Business Owner privalo per dvi darbo dienas po nustatymo eskaluoti nepranešimą apie įtariamą finansų sektoriaus PII incidentą, įrodymų neišsaugojimą, priskirtų veiksmų nevykdymą arba nebendradarbiavimą atliekant pažeidimo vertinimą Privacy Lead / PIMS Manager, o įrodymai turi būti saugomi REG12.

10.1.2 [Both] Incident Response Coordinator privalo per vieną darbo dieną po problemos nustatymo eskaluoti pavėluotą pranešimą, praleistą klasifikavimą, trūkstamus įrodymus, praleistą eskalavimą arba vėluojantį lokalizavimo veiksmą Privacy Lead / PIMS Manager, o įrodymai turi būti saugomi REG10 ir REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager privalo REG12 įrašyti neatitiktį, kai šios politikos pažeidimas paveikia incidento registravimą, pirminį įvertinimą, lokalizavimą, pranešimą, ataskaitų teikimą, įrodymų vientisumą, komunikaciją arba korekcinį veiksmą.

10.1.4 [Both] Vendor / Procurement Owner privalo per penkias darbo dienas inicijuoti tiekėjo, duomenų tvarkytojo, subtvarkytojo arba išorinio paslaugų teikėjo taisomuosius veiksmus per REG08 ir REG12, kai trečioji šalis nevykdo sutartų incidento, pažeidimo, įrodymų arba ataskaitų teikimo pareigų.

10.1.5 [Conditional] Top Management privalo kitos suplanuotos vadovybės peržiūros metu peržiūrėti esmines arba pasikartojančias PII15-FS neatitiktis, o sprendimai ir reikalaujami veiksmai turi būti saugomi REG12.

10.1.6 [All] Privacy Lead / PIMS Manager privalo per 30 kalendorinių dienų REG11 inicijuoti taisomuosius mokymus, kai politikos neatitiktis susijusi su vaidmens informuotumu, pavėluotu pranešimu, eskalavimo nesėkme, įrodymų tvarkymo nesėkme arba komunikacijos nesėkme.

11. Peržiūra ir palaikymas

11.1.1 [Conditional] Privacy Lead / PIMS Manager privalo bent kartą per metus peržiūrėti šią politiką ir REG12 įrašyti peržiūros rezultatą, reikiamus pakeitimus ir patvirtinimo būseną.

11.1.2 [Conditional] Incident Response Coordinator privalo per 30 kalendorinių dienų po bet kurio didelio poveikio finansų sektoriaus PII incidento, patvirtinto PII pažeidimo, reikšmingo finansų sektoriaus incidento arba reikšmingos kibernetinės grėsmės uždarymo inicijuoti šios politikos peržiūrą po incidento, o peržiūros įrodymai turi būti saugomi REG10 ir REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager privalo per 30 kalendorinių dienų po sužinojimo apie esminį teisinių, sektoriaus, klientų, sutartinių, duomenų tvarkytojų, subtvarkytojų, ataskaitų teikimo šablonų, ataskaitų teikimo terminų arba su perdavimu susijusių incidentų ataskaitų teikimo reikalavimų pokytį peržiūrėti šią politiką, o peržiūros įrodymai turi būti saugomi REG01, REG08, REG09 ir REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer privalo bent kartą per metus per PIMS vidaus audito programą peržiūrėti šios politikos įgyvendinimą, o audito išvados ir korekciniai veiksmai turi būti saugomi REG12.

11.1.5 [Conditional] Top Management privalo suplanuotos vadovybės peržiūros metu peržiūrėti incidentų tendencijas, reikšmingus pažeidimus, ataskaitų teikimo veiksmingumą, vėluojančius korekcinius veiksmus ir politikos veiksmingumą, o rezultatai turi būti saugomi REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager privalo bent kartą per metus ir po bet kokio PIMS taikymo srities pakeitimo peržiūrėti PII15-FS ir PII15 pakeitimo santykį, kad patikrintų, jog abi politikos nėra įgyvendinamos tai pačiai finansų sektoriaus taikymo sričiai, o peržiūros įrodymai turi būti saugomi REG03 ir 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 apskaitos ir teisinio pagrindo politika

12.5 PII04 - Privatumo pranešimo ir skaidrumo politika

12.6 PII06 - Duomenų subjektų teisių valdymo politika

12.7 PII07 - Privatumo rizikos vertinimo ir DPIA politika

12.8 PII08 - Privatumo pagal projektavimą ir pagal numatytuosius nustatymus politika

12.9 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika

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

12.11 PII13 - Tarptautinio PII perdavimo politika

12.12 PII14 - PII saugumo ir prieigos kontrolės politika

12.13 PII16 - Privatumo mokymų, informuotumo ir kompetencijos politika

12.14 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika

12.15 PII18 - PIMS stebėsenos, audito ir tobulinimo politika

12.16 PII23 - Debesijos PII duomenų tvarkytojo politika, kai finansų sektoriaus debesijos duomenų tvarkytojo pareigos patenka į taikymo sritį

12.17 PII15 - PII incidentų ir pažeidimų valdymo politika yra bazinė incidentų ir pažeidimų politika. PII15-FS yra finansų sektoriaus PII15 pakeičianti versija. PII15 ir PII15-FS negali būti įgyvendinamos kartu tai pačiai PIMS taikymo sričiai, verslo padaliniui, produktui, kliento aplinkai, reglamentuojamai paslaugai ar įrodymų ribai.

13. Pamatiniai standartai ir sistemos

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].