					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: PII15-FS					Dokumenta nosaukums: **Finanšu sektora personas datu incidentu un pārkāpumu pārvaldības politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/kontrole/pants	Piemērojamība	Pārklājuma veids	Piezīme
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS komunikācija un dokumentēti incidentu pierādījumi
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Darbības kontroles pasākumi, privātuma risku izvērtēšana un sasaiste ar riska apstrādi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Uzraudzība, izvērtēšana, neatbilstība, korektīvā darbība un uzlabošana
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidentu pārvaldības plānošana un sagatavošanās personas datu apstrādei
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reaģēšana uz informācijas drošības incidentiem, kuros iesaistīti personas dati
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Juridiskās, normatīvās, regulatīvās un līgumiskās prasības un ierakstu aizsardzība
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Apstrādātāja klienta vienošanās un atbalsts klienta pienākumu izpildei
GDPR	Article 5(2); Article 24	Controller	Supporting	Pārskatatbildība un pārziņa atbildība

GDPR	Article 26	Joint Controller	Supporting	Kopīgo pārziņu incidentu atbildības koordinācija
GDPR	Article 28	Both	Supporting	Apstrādātāja palīdzība un apstrādātāja līgumiskie pienākumi
GDPR	Article 32	Both	Supporting	Apstrādes drošība un pārkāpumu atklāšanas spēja
GDPR	Article 33	Both	Primary	Paziņošana par personas datu aizsardzības pārkāpumu un pārkāpuma dokumentēšana
GDPR	Article 34	Controller	Primary	Personas datu aizsardzības pārkāpumu paziņošana skartajiem datu subjektiem
GDPR	Article 39	Conditional	Supporting	DPO konsultācijas, uzraudzība, sadarbība un kontaktpunkta atbalsts
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Ar ICT saistītu incidentu pārvaldības process darbības jomā ietilpstošām finanšu vienībām
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Ar ICT saistītu incidentu un nozīmīgu kiberdraudu klasifikācijas kritēriji
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Ziņošana par būtiskiem ar ICT saistītiem incidentiem un paziņošana par

				nozīmīgiem kiberdraudiem
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Ziņojumu saturs, termiņi, veidnes un procedūras
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Ziņošana par būtiskiem incidentiem, ja piemērojams
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informācijas drošības un privātuma atbilstības principi
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Personas datu incidentu reaģēšanas pienākumi un ziņošana par notikumiem
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentu plānošana, izvērtēšana, reaģēšana, gūtās mācības un pierādījumu vākšana
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Incidentu pārvaldības procesa dzīves cikls
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentu politika, plāns, informētība, testēšana un gūtās mācības
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Atklāšanas, paziņošanas, triāžas, analīzes, reaģēšanas un ziņošanas operācijas
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Publiskā mākoņa apstrādātāja paziņošanas un pārkāpumu ierakstu gaidas

1. Piemērošanas joma

1.1 Šī politika nosaka prasības personas datu incidentu un personas datu aizsardzības pārkāpumu identificēšanai, ziņošanai, triāžai, klasificēšanai, izvērtēšanai, ierobežošanai, paziņošanai, dokumentēšanai, slēgšanai un uzlabošanai finanšu sektora PIMS darbības jomās.

1.2 **Ieviešanas paziņojums:** Šī politika ir PII15 aizstājējvariants finanšu sektoram. To nedrīkst ieviest vienlaikus ar PII15 tai pašai PIMS darbības jomai, struktūrvienībai, produktam, klienta videi, regulētam pakalpojumam vai pierādījumu robežai. Organizācijām tai pašai darbības jomai jāizvēlas vai nu PII15, vai PII15-FS, lai izvairītos no dublētiem incidentu pārvaldības pienākumiem, dublētiem reģistriem un dublēta audita pierādījumu darba.

1.3 Šī politika attiecas uz:

1.3.1 organizāciju, kas finanšu sektora kontekstā darbojas kā personas datu pārzinis;

1.3.2 organizāciju, kas darbojas kā kopīgs pārzinis, ja nepieciešama incidentu vai pārkāpumu atbildības koordinācija;

1.3.3 organizāciju, kas finanšu sektora klientiem darbojas kā personas datu apstrādātājs;

1.3.4 organizāciju, kas finanšu sektora klientiem vai augšupējiem apstrādātājiem darbojas kā apakšapstrādātājs;

1.3.5 sistēmām, lietojumprogrammām, pakalpojumiem, procesiem, piegādātājiem, apstrādātājiem, apakšapstrādātājiem un trešajām pusēm, kas finanšu sektora PIMS darbības jomā apstrādā, glabā, pārsūta, atbalsta, piekļūst vai citādi ietekmē personas datus.

1.4 Šī politika izmanto REG10 - Personas datu incidentu un pārkāpumu reģistru kā primāro pierādījumu objektu finanšu sektora personas datu incidentu un pārkāpumu pārvaldībai.

1.5 Šī politika izmanto atbalsta pierādījumu objektus šādi:

1.5.1 REG01 PIMS darbības jomai, piemērojamo ieinteresēto pušu, nozares, klientu, līgumiskajam un ziņošanas kontekstam.

1.5.2 REG02 skartajām apstrādes darbībām, personas datu kategorijām, datu subjektu kategorijām, nolūkiem, sistēmām un pakalpojumiem.

1.5.3 REG03 Piemērojamības paziņojumam un kontroles pasākumu piemērojamības atjauninājumiem, tostarp PII15 aizstāšanai ar PII15-FS tai pašai darbības jomai.

1.5.4 REG04 privātuma riskam, DPIA, atlikušajam riskam un sasaistei ar riska apstrādi.

1.5.5 REG08 apstrādātāja, apakšapstrādātāja, klienta, piegādātāja un trešās puses incidentu saskarnes pierādījumiem.

1.5.6 REG09 starptautiskas nosūtīšanas sasaistei, ja incidents ietekmē pārrobežu apstrādi.

1.5.7 REG11 apmācības, informētības un incidentu reaģēšanas kompetences pierādījumiem.

1.5.8 REG12 audita, neatbilstības, korektīvās darbības, vadības pārskatīšanas un uzlabošanas pierādījumiem.

1.6 Šī politika balstās uz saistītajām PIMS politikām specializētiem kontroles pasākumiem:

1.6.1 PII03 nosaka apstrādes uzskaites un tiesiskā pamata ierakstu pārvaldību.

1.6.2 PII04 nosaka privātuma paziņojumu un pārredzamības kontroles pasākumus ārpus pārkāpumiem specifiskas komunikācijas.

1.6.3 PII06 nosaka datu subjektu tiesību īstenošanas pieprasījumus, kas rodas pirms incidenta, tā laikā vai pēc tā.

1.6.4 PII07 nosaka privātuma risku izvērtēšanas un DPIA metodoloģiju.

1.6.5 PII08 nosaka datu aizsardzību pēc projektēšanas un pēc noklusējuma.

1.6.6 PII10 nosaka glabāšanas, dzēšanas un likvidēšanas kontroles pasākumus.

1.6.7 PII12 nosaka apstrādātāju, apakšapstrādātāju, piegādātāju un trešo pušu privātuma attiecību kontroles pasākumus.

1.6.8 PII13 nosaka starptautisku personas datu nosūtīšanas mehānismus un nosūtīšanas riska ierakstus.

1.6.9 PII14 nosaka preventīvus un atklājošus personas datu drošības un piekļuves kontroles pasākumus.

1.6.10 PII16 nosaka privātuma apmācību, informētību un kompetenci.

1.6.11 PII17 nosaka dokumentētas informācijas un pierādījumu pārvaldību.

1.6.12 PII18 nosaka uzraudzību, iekšējo auditu, vadības pārskatīšanu, neatbilstību, korektīvo darbību un nepārtrauktu uzlabošanu.

1.6.13 PII23 nosaka mākoņpakalpojumu personas datu apstrādātāja kontroles pasākumus, ja darbības jomā ietilpst mākoņapstrādātāja pienākumi.

1.7 Šīs politikas izpratnē:

1.7.1 “Personas datu incidents” ir aizdomīgs vai apstiprināts notikums, kas ir ietekmējis, varētu būt ietekmējis vai pamatoti var ietekmēt personas datu konfidencialitāti, integritāti, pieejamību, likumīgu apstrādi vai autorizētu apstrādi.

1.7.2 “Personas datu aizsardzības pārkāpums” ir apstiprināts personas datu incidents, kas ietver nesankcionētu, nelikumīgu, nejaušu vai neparedzētu personas datu iznīcināšanu, nozaudēšanu, izmainīšanu, izpaušanu, piekļuvi tiem, nepieejamību vai kompromitēšanu.

1.7.3 “Finanšu sektora personas datu incidents” ir personas datu incidents, kas ietekmē, var ietekmēt vai ir pamatoti saistīts ar regulētiem finanšu pakalpojumiem, finanšu sektora klientiem, finanšu darījumu partneriem, finanšu darījumiem, finanšu operācijām vai finanšu sektora personas datu apstrādi.

1.7.4 “Būtisks finanšu sektora incidents” ir finanšu sektora personas datu incidents vai saistīts ICT incidents, kas atbilst REG10 dokumentētajiem būtiskuma vai ziņošanas kritērijiem.

1.7.5 “Nozīmīgs kiberdrauds” ir REG10 ierakstīts kiberdrauds, kas var būtiski ietekmēt darbības jomā ietilpstošus finanšu sektora pakalpojumus, personas datu apstrādi, klientus, darījumu partnerus vai operācijas.

1.7.6 “Pārkāpuma izvērtēšana” ir dokumentēts izvērtējums par to, vai personas datu incidents ir personas datu aizsardzības pārkāpums, kādi personas dati un datu subjekti ir skarti, kādi riski var rasties, kādi paziņojumi vai komunikācija ir nepieciešami un kādas korektīvās darbības ir vajadzīgas.

1.7.7 “Apzināšanās” ir brīdis, kad organizācijai ir pamatota pārliecības pakāpe, ka ir noticis drošības vai privātuma incidents un personas dati ir vai varētu būt kompromitēti.

1.7.8 “Augstas ietekmes finanšu sektora personas datu incidents” ir personas datu incidents, kas ietver augsta riska apstrādi, īpašu kategoriju personas datus vai ļoti sensitīvus personas datus, liela mēroga personas datus, neaizsargātas personas, regulētus klientus, būtisku pakalpojuma darbības traucējumu, finanšu darījumu partnerus, finanšu darījumus, vairāku jurisdikciju ietekmi, privileģētas piekļuves kompromitēšanu, publisku ekspozīciju, izspiedējprogrammatūru, pakalpojuma nepieejamību vai būtisku operacionālu, klientu, finansiālu vai reputācijas ietekmi.

1.7.9 “Būtiska izmaiņa incidentā” ir jauna vai mainīta informācija, kas ietekmē incidenta tvērumu, smaguma pakāpi, personas datu kategorijas, ietekmi uz datu subjektiem, pakalpojuma ietekmi, finanšu sektora klasifikāciju, paziņošanas lēmumu, klientu ietekmi, pamatcēloni, ierobežošanu, atjaunošanu, korektīvo darbību vai ārējās ziņošanas pienākumus.

2. Mērķis

2.1 Šīs politikas mērķis ir nodrošināt, ka personas datu incidenti un pārkāpumi finanšu sektora kontekstos tiek apstrādāti konsekventi, savlaicīgi, likumīgi, droši un ar auditam gataviem pierādījumiem.

2.2 Šī politika atbalsta pārskatatbildību, prasot finanšu sektora personas datu incidentus un pārkāpumus ierakstīt REG10 un sasaistīt ar skartajiem apstrādes ierakstiem, privātuma riskiem, apstrādātāju un apakšapstrādātāju attiecībām, nosūtīšanas ierakstiem, korektīvajām darbībām, apmācību ierakstiem, finanšu sektora ziņošanas lēmumiem un vadības pārskatīšanas pierādījumiem, ja tie tiek aktivizēti.

2.3 Šī politika nodrošina, ka pārziņa, kopīga pārziņa, apstrādātāja un apakšapstrādātāja pienākumi tiek apstrādāti, izmantojot atšķirīgus piemērojamības noteikumus, vienlaikus saglabājot vienotu integrētu finanšu sektora incidentu un pārkāpumu pierādījumu modeli.

3. Mērķi

3.1 Šīs politikas mērķi ir:

3.1.1 nodrošināt, ka aizdomīgi finanšu sektora personas datu incidenti tiek ziņoti un reģistrēti savlaicīgi;

3.1.2 nodrošināt, ka finanšu sektora personas datu incidenti tiek triāžēti un klasificēti, izmantojot konsekventus privātuma, drošības, darbības un nozares kritērijus;

3.1.3 nodrošināt, ka pārkāpuma izvērtēšanā tiek ņemti vērā skartie personas dati, datu subjekti, sistēmas, pakalpojumi, apstrādes darbības, apstrādātāji, apakšapstrādātāji, nosūtīšanas, riski, klienti, darījumu partneri un korektīvās darbības;

3.1.4 nodrošināt, ka pārziņa paziņošanas un datu subjektu komunikācijas lēmumi tiek dokumentēti;

3.1.5 nodrošināt, ka apstrādātāja un apakšapstrādātāja paziņojumi par pārkāpumu klientiem vai augšupējām pusēm tiek sniegti bez nepamatotas kavēšanās un saskaņā ar piemērojamām vienošanām;

3.1.6 nodrošināt, ka finanšu sektora ziņošanas trigeri tiek izvērtēti, dokumentēti un izsekoti, ja piemērojams;

3.1.7 nodrošināt, ka pierādījumi incidenta apstrādes laikā tiek saglabāti un aizsargāti;

3.1.8 nodrošināt, ka ierobežošana, izskaušana, atjaunošana un validācija tiek izsekota REG10;

3.1.9 nodrošināt, ka nozīmīgi kiberdraudi un būtiski finanšu sektora incidenti tiek novirzīti uz atbilstošām lēmumu un ziņošanas darbplūsmām;

3.1.10 nodrošināt, ka incidentos gūtās mācības rezultējas korektīvā darbībā, apmācībā, kontroles pasākumu uzlabošanā un vadības pārskatīšanā;

3.1.11 nodrošināt, ka incidentu un pārkāpumu ieraksti ir pieejami auditam, vadības pārskatīšanai, klientu apliecinājumam un regulatīvai pārskatīšanai, ja piemērojams;

3.1.12 nodrošināt, ka PII15-FS aizstāj PII15 tai pašai finanšu sektora darbības jomai un nedublē PII15 pierādījumu darbu.

4. Politikas paziņojumi

4.1 Varianta aktivizēšana, gatavība un saņemšana

4.1.1 [Conditional] Privacy Lead / PIMS Manager ir jādokumentē PII15-FS aktivizēšana REG01 un REG03, pirms šī politika tiek izmantota finanšu sektora PIMS darbības jomai.

4.1.2 [Conditional] Privacy Lead / PIMS Manager pirms PII15-FS apstiprināšanas REG03 un REG12 ir jādokumentē, ka PII15 netiek vienlaikus ieviesta tai pašai finanšu sektora PIMS darbības jomai.

4.1.3 [All] Incident Response Coordinator katrs ziņotais vai atklātais aizdomīgais finanšu sektora personas datu incidents jāieraksta REG10 vienas darbdienas laikā pēc saņemšanas vai agrāk, ja var tikt aktivizēts piemērojams paziņošanas, klienta vai ziņošanas termiņš.

4.1.4 [Conditional] Privacy Lead / PIMS Manager vismaz reizi gadā un pēc jebkādām būtiskām izmaiņām PIMS darbības jomā, tiesiskajā kontekstā, klientu pienākumos, līgumiskajos pienākumos, nozares ziņošanas kontekstā vai augsta riska apstrādē REG10 jāuztur finanšu sektora personas datu incidentu un pārkāpumu apstrādes kritēriji.

4.1.5 [Both] Information Security Lead 24 stundu laikā pēc tam, kad aizdomīgs incidents ietekmē sistēmu, pakalpojumu vai lietojumprogrammu, kas apstrādā personas datus, REG10 jāapstiprina incidenta pierādījumu saglabāšanas prasības.

4.1.6 [Conditional] Vendor / Procurement Owner pirms uzņemšanas un vismaz reizi gadā darbības jomā ietilpstošiem apstrādātājiem, apakšapstrādātājiem, piegādātājiem un ārpakalpojuma ziņošanas pakalpojumu sniedzējiem REG08 jāuztur finanšu sektora trešo pušu incidentu kontaktinformācijas un pierādījumu maršrutēšanas prasības.

4.2 Klasifikācija un pārkāpuma izvērtēšana

4.2.1 [All] Incident Response Coordinator katrs REG10 ieraksts 24 stundu laikā pēc saņemšanas jāklasificē kā notikums, kas nav personas datu notikums, aizdomīgs personas datu incidents, apstiprināts personas datu incidents, apstiprināts personas datu aizsardzības pārkāpums, finanšu sektora personas datu incidents, būtisks finanšu sektora incidents, nozīmīgs kiberdrauds vai ieraksts ar gaidāmu klasifikāciju.

4.2.2 [Conditional] Information Security Lead REG10 jāizvērtē skartie pakalpojumi, klienti, darījumu partneri, darījumi, pakalpojuma dīkstāve, ģeogrāfiskā izplatība, datu zudums, pakalpojuma kritiskums un ekonomiskā ietekme, ja personas datu incidents var ietekmēt finanšu sektora pakalpojumus vai operācijas.

4.2.3 [Both] Privacy Lead / PIMS Manager pirms pārkāpuma paziņošanas lēmuma pabeigšanas REG02, REG04, REG08, REG09 un REG10 jāidentificē skartā apstrādes darbība, personas datu kategorijas, datu subjektu kategorijas, sistēmas, apstrādātāji, apakšapstrādātāji, nosūtīšanas vietas un privātuma riski.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor katram apstiprinātam vai pamatoti aizdomīgam personas datu aizsardzības pārkāpumam jāizvērtē risks skartajiem datu subjektiem un pirms ārējā paziņošanas lēmuma pieņemšanas REG10 jāieraksta paziņošanas ieteikums, riska pamatojums un konsultācija.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager 24 stundu laikā pēc kopīgas atbildības par aizdomīgu vai apstiprinātu personas datu aizsardzības pārkāpumu identificēšanas REG08 un REG10 jāieraksta kopīgo pārziņu incidenta atbildības sadalījums.

4.2.6 [Processor] Privacy Lead / PIMS Manager 24 stundu laikā pēc tam, kad aizdomīgs vai apstiprināts personas datu aizsardzības pārkāpums ietekmē apstrādi, kas veikta apstrādātāja statusā, REG08 un REG10 jāizvērtē klienta norādījumi, līgumiskie paziņošanas pienākumi un sadarbības pienākumi.

4.2.7 [Subprocessor] Vendor / Procurement Owner 24 stundu laikā pēc tam, kad aizdomīgs vai apstiprināts personas datu incidents ietekmē apstrādi, kas veikta apakšapstrādātāja statusā, REG08 un REG10 jāidentificē augšupējā paziņošanas ķēde un nepieciešamā pierādījumu maršrutēšana.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Izņēmumi

9.1.1 [All] Privacy Lead / PIMS Manager jebkurš izņēmums no šīs politikas jāieraksta REG12 pirms ieviešanas vai 24 stundu laikā pēc ārkārtas darbības, ja iepriekšēja apstiprināšana nebija iespējama.

9.1.2 [Conditional] Top Management pirms incidenta slēgšanas jāapstiprina jebkurš izņēmums, kas būtiski ietekmē pārkāpuma paziņošanas laiku, finanšu sektora ziņošanas laiku, publisku komunikāciju, klienta apņemšanos, pierādījumu saglabāšanu vai risku datu subjektiem, apstiprinājuma pierādījumus saglabājot REG10 un REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor pirms incidenta slēgšanas jādokumentē konsultācijas par jebkuru kavētu paziņošanu, nepaziņošanas lēmumu, ziņošanas izņēmumu vai ārkārtas komunikācijas pieeju, konsultācijas saglabājot REG10.

9.1.4 [Both] Vendor / Procurement Owner piecu darbdienu laikā pēc izņēmuma identificēšanas REG08 un REG12 jāieraksta piegādātāja, apstrādātāja, apakšapstrādātāja, klienta vai ārpakalpojuma sniedzēja izņēmumi, kas ietekmē finanšu sektora incidentu reaģēšanu.

9.1.5 [All] Privacy Lead / PIMS Manager vismaz reizi mēnesī līdz slēgšanai jāpārskata atvērtie izņēmumi no šīs politikas, pārskatīšanas statusu saglabājot REG12.

10. Ievērošana

10.1.1 [All] Process Owner / Business Owner divu darbdienu laikā pēc atklāšanas jāeskalē Privacy Lead / PIMS Manager nespēja ziņot par aizdomīgu finanšu sektora personas datu incidentu, saglabāt pierādījumus, izpildīt piešķirtās darbības vai sadarboties pārkāpuma izvērtēšanā, pierādījumus saglabājot REG12.

10.1.2 [Both] Incident Response Coordinator vienas darbdienas laikā pēc problēmas identificēšanas jāeskalē Privacy Lead / PIMS Manager novēlota ziņošana, nokavēta klasifikācija, trūkstoši pierādījumi, nokavēta eskalācija vai nokavēta ierobežošanas darbība, pierādījumus saglabājot REG10 un REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager jāieraksta REG12 neatbilstība, ja šīs politikas pārkāpums ietekmē incidenta saņemšanu, triāžu, ierobežošanu, paziņošanu, ziņošanu, pierādījumu integritāti, komunikāciju vai korektīvo darbību.

10.1.4 [Both] Vendor / Procurement Owner piecu darbdienu laikā caur REG08 un REG12 jāuzsāk piegādātāja, apstrādātāja, apakšapstrādātāja vai ārpakalpojuma sniedzēja trūkumu novēršana, ja trešā puse neizpilda saskaņotos incidentu, pārkāpumu, pierādījumu vai ziņošanas pienākumus.

10.1.5 [Conditional] Top Management nākamajā plānotajā vadības pārskatīšanā jāpārskata būtiskas vai atkārtotas PII15-FS neatbilstības, lēmumus un nepieciešamās darbības saglabājot REG12.

10.1.6 [All] Privacy Lead / PIMS Manager 30 kalendāro dienu laikā REG11 jāaktivizē koriģējoša apmācība, ja politikas neatbilstība ietver lomas informētību, novēlotu ziņošanu, eskalācijas neizpildi, pierādījumu apstrādes kļūmi vai komunikācijas kļūmi.

11. Pārskatīšana un uzturēšana

11.1.1 [Conditional] Privacy Lead / PIMS Manager vismaz reizi gadā jāpārskata šī politika un REG12 jāieraksta pārskatīšanas rezultāts, nepieciešamās izmaiņas un apstiprinājuma statuss.

11.1.2 [Conditional] Incident Response Coordinator 30 kalendāro dienu laikā pēc jebkura augstas ietekmes finanšu sektora personas datu incidenta, apstiprināta personas datu aizsardzības pārkāpuma, būtiska finanšu sektora incidenta vai nozīmīga kiberdrauda slēgšanas jāaktivizē šīs politikas pēcincidenta pārskatīšana, pārskatīšanas pierādījumus saglabājot REG10 un REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager 30 kalendāro dienu laikā pēc tam, kad kļuvis zināms par būtiskām izmaiņām juridiskajās, nozares, klienta, līgumiskajās, apstrādātāja, apakšapstrādātāja, ziņošanas veidņu, ziņošanas termiņu vai ar nosūtīšanu saistītajās incidentu ziņošanas prasībās, jāpārskata šī politika, pārskatīšanas pierādījumus saglabājot REG01, REG08, REG09 un REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer vismaz reizi gadā PIMS iekšējā audita programmas ietvaros jāpārskata šīs politikas ieviešana, audita konstatējumus un korektīvās darbības saglabājot REG12.

11.1.5 [Conditional] Top Management plānotās vadības pārskatīšanas laikā jāpārskata incidentu tendences, būtiski pārkāpumi, ziņošanas veiktspēja, nokavētās korektīvās darbības un politikas efektivitāte, rezultātus saglabājot REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager vismaz reizi gadā un pēc jebkādām PIMS darbības jomas izmaiņām jāpārskata aizstāšanas attiecība starp PII15-FS un PII15, lai pārliecinātos, ka abas politikas netiek ieviestas tai pašai finanšu sektora darbības jomai, pārskatīšanas pierādījumus saglabājot REG03 un REG12.

12. Saistītās politikas

12.1 Šī politika jālasa kopā ar:

12.1.1 PII01 - Privātuma informācijas pārvaldības sistēmas politika

12.1.2 PII02 - Privātuma lomu, pienākumu un pārskatatbildības politika

12.1.3 PII03 - Personas datu apstrādes uzskaites un tiesiskā pamata politika

12.1.4 PII04 - Privātuma paziņojumu un pārredzamības politika

12.1.5 PII06 - Datu subjektu tiesību pārvaldības politika

12.1.6 PII07 - Privātuma risku izvērtēšanas un DPIA politika

12.1.7 PII08 - Datu aizsardzības pēc projektēšanas un pēc noklusējuma politika

12.1.8 PII10 - Personas datu glabāšanas, dzēšanas un likvidēšanas politika

12.1.9 PII12 - Apstrādātāju, apakšapstrādātāju un trešo pušu privātuma pārvaldības politika

12.1.10 PII13 - Starptautiskas personas datu nosūtīšanas politika

12.1.11 PII14 - Personas datu drošības un piekļuves kontroles politika

12.1.12 PII16 - Privātuma apmācības, informētības un kompetences politika

12.1.13 PII17 - PIMS dokumentētās informācijas un pierādījumu pārvaldības politika

12.1.14 PII18 - PIMS uzraudzības, audita un uzlabošanas politika

12.1.15 PII23 - Mākoņpakalpojumu personas datu apstrādātāja politika, ja darbības jomā ietilpst finanšu sektora mākoņapstrādātāja pienākumi

12.2 PII15 - Personas datu incidentu un pārkāpumu pārvaldības politika ir pamata incidentu un pārkāpumu politika. PII15-FS ir PII15 aizstājējvariants finanšu sektoram. PII15 un PII15-FS nedrīkst ieviest vienlaikus tai pašai PIMS darbības jomai, struktūrvienībai, produktam, klienta videi, regulētam pakalpojumam vai pierādījumu robežai.

13. Atsauces standarti un ietvari

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].