					Sem vložte název registrované právnické osoby						
Číslo dokumentu: PII15-FS					Název dokumentu: **Politika řízení incidentů PII a porušení zabezpečení PII ve finančním sektoru**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikace PIMS a dokumentované důkazy o incidentech
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativní řízení, posouzení rizik pro soukromí a vazba na ošetření rizik
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování, hodnocení, neshody, nápravná opatření a zlepšování
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Plánování a příprava řízení incidentů pro zpracování PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reakce na incidenty informační bezpečnosti týkající se PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Právní, zákonné, regulační a smluvní požadavky a ochrana záznamů
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Smlouva se zákazníkem zpracovatele a podpora povinností zákazníka
GDPR	Article 5(2); Article 24	Controller	Supporting	Odpovědnost a odpovědnost správce
GDPR	Article 26	Joint Controller	Supporting	Koordinace odpovědnosti společných správců při incidentech
GDPR	Article 28	Both	Supporting	Součinnost zpracovatele a smluvní povinnosti zpracovatele

GDPR	Article 32	Both	Supporting	Zabezpečení zpracování a schopnost detekce porušení zabezpečení
GDPR	Article 33	Both	Primary	Oznamování porušení zabezpečení osobních údajů a dokumentace porušení zabezpečení
GDPR	Article 34	Controller	Primary	Informování dotčených subjektů PII o porušení zabezpečení osobních údajů
GDPR	Article 39	Conditional	Supporting	Poradenství DPO, monitorování, spolupráce a podpora kontaktního místa
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces řízení incidentů souvisejících s ICT pro finanční subjekty v rozsahu působnosti
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Klasifikační kritéria pro incidenty související s ICT a významné kybernetické hrozby
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Hlášení závažných incidentů souvisejících s ICT a oznamování významných kybernetických hrozeb
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Obsah hlášení, lhůty, šablony a postupy
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Hlášení významných incidentů, je-li použitelné

ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zásady bezpečnosti informací a souladu v oblasti soukromí
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odpovědnosti při reakci na incidenty týkající se PII a hlášení událostí
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Plánování incidentů, posouzení, reakce, získané poznatky a sběr důkazů
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životní cyklus procesu řízení incidentů
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, plán, povědomí, testování a získané poznatky v oblasti incidentů
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detekce, oznamování, triáž, analýza, reakce a provozní hlášení
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očekávání ohledně oznamování zpracovatelem ve veřejném cloudu a záznamů o porušení zabezpečení

1. Rozsah

1.1 Tato politika stanoví požadavky na identifikaci, hlášení, triáž, klasifikaci, posuzování, zamezení šíření, oznamování, dokumentování, uzavírání a zlepšování na základě incidentů týkajících se PII a porušení zabezpečení osobních údajů v rozsazích PIMS ve finančním sektoru.

1.2 **Upozornění k implementaci:** Tato politika je náhradní variantou PII15 pro finanční sektor. Nesmí být implementována souběžně s PII15 pro stejný rozsah PIMS, obchodní jednotku, produkt, zákaznické prostředí, regulovanou službu nebo hranici důkazů. Organizace musí pro stejný rozsah zvolit buď PII15, nebo PII15-FS, aby se zabránilo duplicitním povinnostem řízení incidentů, duplicitním registrům a duplicitní práci s auditními důkazy.

1.3 Tato politika se vztahuje na:

1.3.1 organizaci jednající jako správce PII v kontextu finančního sektoru;

1.3.2 organizaci jednající jako společný správce, pokud je vyžadována koordinace odpovědnosti za incident nebo porušení zabezpečení;

1.3.3 organizaci jednající jako zpracovatel PII pro zákazníky z finančního sektoru;

1.3.4 organizaci jednající jako dílčí zpracovatel pro zákazníky z finančního sektoru nebo nadřazené zpracovatele;

1.3.5 systémy, aplikace, služby, procesy, dodavatele, zpracovatele, dílčí zpracovatele a třetí strany, které v rámci rozsahu PIMS pro finanční sektor zpracovávají, ukládají, přenášejí, podporují, zpřístupňují nebo jinak ovlivňují PII.

1.4 Tato politika používá REG10 - Registr incidentů PII a porušení zabezpečení PII jako hlavní důkazní objekt pro řízení incidentů PII a porušení zabezpečení PII ve finančním sektoru.

1.5 Tato politika používá podpůrné důkazní objekty takto:

1.5.1 REG01 pro rozsah PIMS, použitelné zainteresované strany a odvětvový, zákaznický, smluvní a oznamovací kontext.

1.5.2 REG02 pro dotčené činnosti zpracování, kategorie PII, kategorie subjektů PII, účely, systémy a služby.

1.5.3 REG03 pro Prohlášení o použitelnosti a aktualizace použitelnosti opatření, včetně nahrazení PII15 politikou PII15-FS pro stejný rozsah.

1.5.4 REG04 pro vazbu na rizika pro soukromí, DPIA, zbytkové riziko a ošetření rizik.

1.5.5 REG08 pro důkazy o rozhraních pro incidenty se zpracovateli, dílčími zpracovateli, zákazníky, dodavateli a třetími stranami.

1.5.6 REG09 pro vazbu na mezinárodní předávání, pokud incident ovlivňuje přeshraniční zpracování.

1.5.7 REG11 pro důkazy o školení, povědomí a kompetencích k reakci na incidenty.

1.5.8 REG12 pro důkazy o auditu, neshodách, nápravných opatřeních, přezkoumání vedením a zlepšování.

1.6 Tato politika se u specializovaných opatření opírá o související politiky PIMS:

1.6.1 PII03 upravuje evidenci činností zpracování a záznamy o právních základech.

1.6.2 PII04 upravuje oznámení o ochraně osobních údajů a opatření transparentnosti mimo komunikaci specifickou pro porušení zabezpečení.

1.6.3 PII06 upravuje žádosti subjektů PII o uplatnění práv, které vzniknou před incidentem, během něj nebo po něm.

1.6.4 PII07 upravuje metodiku posouzení rizik pro soukromí a DPIA.

1.6.5 PII08 upravuje ochranu osobních údajů již od návrhu a ve výchozím nastavení.

1.6.6 PII10 upravuje uchovávání, výmaz a likvidaci.

1.6.7 PII12 upravuje vztahy se zpracovateli, dílčími zpracovateli, dodavateli a třetími stranami v oblasti ochrany soukromí.

1.6.8 PII13 upravuje mechanismy mezinárodního předávání PII a záznamy o rizicích předávání.

1.6.9 PII14 upravuje preventivní a detekční bezpečnostní opatření a řízení přístupu pro PII.

1.6.10 PII16 upravuje školení, povědomí a kompetence v oblasti ochrany soukromí.

1.6.11 PII17 upravuje dokumentované informace a správu důkazů.

1.6.12 PII18 upravuje monitorování, interní audit, přezkoumání vedením, neshody, nápravná opatření a neustálé zlepšování.

1.6.13 PII23 upravuje opatření zpracovatele PII v cloudu, pokud jsou povinnosti cloudového zpracovatele v rozsahu.

1.7 Pro účely této politiky:

1.7.1 „incident týkající se PII“ znamená podezřelou nebo potvrzenou událost, která ovlivnila, mohla ovlivnit nebo by přiměřeně mohla ovlivnit důvěrnost, integritu, dostupnost, zákonné zpracování nebo oprávněné nakládání s PII.

1.7.2 „porušení zabezpečení osobních údajů“ znamená potvrzený incident týkající se PII zahrnující neoprávněné, nezákonné, náhodné nebo nezamýšlené zničení, ztrátu, změnu, zpřístupnění, přístup k, nedostupnost nebo kompromitaci PII.

1.7.3 „incident týkající se PII ve finančním sektoru“ znamená incident týkající se PII, který ovlivňuje, může ovlivnit nebo je přiměřeně spojen s regulovanými finančními službami, zákazníky z finančního sektoru, finančními protistranami, finančními transakcemi, finančními operacemi nebo zpracováním PII ve finančním sektoru.

1.7.4 „závažný incident ve finančním sektoru“ znamená incident týkající se PII ve finančním sektoru nebo související incident ICT, který splňuje dokumentovaná kritéria významnosti nebo hlášení v REG10.

1.7.5 „významná kybernetická hrozba“ znamená kybernetickou hrozbu zaznamenanou v REG10, která by mohla významně ovlivnit finanční služby, zpracování PII, zákazníky, protistrany nebo operace v rozsahu.

1.7.6 „posouzení porušení zabezpečení osobních údajů“ znamená dokumentované vyhodnocení, zda je incident týkající se PII porušením zabezpečení osobních údajů, jaké PII a subjekty PII jsou dotčeny, jaká rizika mohou vzniknout, jaká oznámení nebo komunikace jsou vyžadovány a jaké nápravné opatření je potřebné.

1.7.7 „vědomost“ znamená okamžik, kdy má organizace přiměřenou míru jistoty, že došlo k bezpečnostnímu incidentu nebo incidentu v oblasti soukromí a že PII byly nebo mohly být kompromitovány.

1.7.8 „incident s významným dopadem týkající se PII ve finančním sektoru“ znamená incident týkající se PII zahrnující vysoce rizikové zpracování, zvláštní kategorie nebo vysoce citlivé PII, rozsáhlé PII, zranitelné osoby, regulované zákazníky, významné narušení služby, finanční protistrany, finanční transakce, dopad ve více jurisdikcích, kompromitaci privilegovaného přístupu, veřejnou expozici, ransomware, nedostupnost služby nebo významný provozní, zákaznický, finanční či reputační dopad.

1.7.9 „významná změna incidentu“ znamená nové nebo změněné informace ovlivňující rozsah incidentu, závažnost, kategorie PII, dopad na subjekty PII, dopad na služby, klasifikaci pro finanční sektor, rozhodnutí o oznámení, dopad na zákazníky, kořenovou příčinu, zamezení šíření, obnovu, nápravné opatření nebo povinnosti externího hlášení.

2. Účel

2.1 Účelem této politiky je zajistit, aby incidenty týkající se PII a porušení zabezpečení osobních údajů ve finančním sektoru byly řešeny konzistentně, neprodleně, zákonně, bezpečně a s důkazy připravenými pro audit.

2.2 Tato politika podporuje odpovědnost tím, že vyžaduje, aby incidenty týkající se PII a porušení zabezpečení osobních údajů ve finančním sektoru byly zaznamenány v REG10 a propojeny s dotčenými záznamy o zpracování, riziky pro soukromí, vztahy se zpracovateli a dílčími zpracovateli, záznamy o předávání, nápravnými opatřeními, záznamy o školení, rozhodnutími o hlášení ve finančním sektoru a důkazy o přezkoumání vedením, pokud jsou aktivovány.

2.3 Tato politika zajišťuje, aby povinnosti správce, společného správce, zpracovatele a dílčího zpracovatele byly řešeny prostřednictvím odlišných pravidel použitelnosti při zachování jednoho integrovaného modelu důkazů pro incidenty a porušení zabezpečení ve finančním sektoru.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 zajistit, aby podezřelé incidenty týkající se PII ve finančním sektoru byly neprodleně hlášeny a zaznamenávány;

3.1.2 zajistit, aby incidenty týkající se PII ve finančním sektoru byly tříděny a klasifikovány podle konzistentních kritérií ochrany soukromí, bezpečnosti, provozu a odvětví;

3.1.3 zajistit, aby posouzení porušení zabezpečení zohledňovala dotčené PII, subjekty PII, systémy, služby, činnosti zpracování, zpracovatele, dílčí zpracovatele, předávání, rizika, zákazníky, protistrany a nápravná opatření;

3.1.4 zajistit dokumentování rozhodnutí o oznámení správcem a komunikaci se subjekty PII;

3.1.5 zajistit, aby zpracovatelé a dílčí zpracovatelé oznamovali porušení zabezpečení zákazníkům nebo nadřazeným stranám bez zbytečného odkladu a v souladu s použitelnými smlouvami;

3.1.6 zajistit, aby byly vyhodnoceny, dokumentovány a sledovány spouštěče hlášení ve finančním sektoru, jsou-li použitelné;

3.1.7 zajistit uchování a ochranu důkazů během řešení incidentu;

3.1.8 zajistit, aby zamezení šíření, eradikace, obnova a validace byly sledovány prostřednictvím REG10;

3.1.9 zajistit, aby významné kybernetické hrozby a závažné incidenty ve finančním sektoru byly směrovány do příslušných rozhodovacích a oznamovacích pracovních postupů;

3.1.10 zajistit, aby získané poznatky z incidentů vedly k nápravným opatřením, školení, zlepšení opatření a přezkoumání vedením;

3.1.11 zajistit, aby záznamy o incidentech a porušeních zabezpečení byly dostupné pro audit, přezkoumání vedením, ujištění zákazníků a regulační přezkum, je-li použitelný;

3.1.12 zajistit, aby PII15-FS nahradila PII15 pro stejný rozsah finančního sektoru a neduplikovala práci s důkazy podle PII15.

4. Prohlášení politiky

4.1 Aktivace varianty, připravenost a příjem hlášení

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUSÍ před použitím této politiky pro rozsah PIMS ve finančním sektoru dokumentovat aktivaci PII15-FS v REG01 a REG03.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUSÍ před schválením PII15-FS dokumentovat v REG03 a REG12, že PII15 není souběžně implementována pro stejný rozsah PIMS ve finančním sektoru.

4.1.3 [All] Incident Response Coordinator MUSÍ zaznamenat každý nahlášený nebo detekovaný podezřelý incident týkající se PII ve finančním sektoru do REG10 do jednoho pracovního dne od přijetí, nebo dříve, pokud může být aktivována použitelná oznamovací, zákaznická nebo vykazovací lhůta.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUSÍ udržovat kritéria pro řešení incidentů týkajících se PII a porušení zabezpečení PII ve finančním sektoru v REG10 alespoň jednou ročně a po jakékoli významné změně rozsahu PIMS, právního kontextu, povinností vůči zákazníkům, smluvních povinností, odvětvového oznamovacího kontextu nebo vysoce rizikového zpracování.

4.1.5 [Both] Information Security Lead MUSÍ potvrdit požadavky na uchování důkazů o incidentu v REG10 do 24 hodin poté, co podezřelý incident ovlivní systém, službu nebo aplikaci zpracovávající PII.

4.1.6 [Conditional] Vendor / Procurement Owner MUSÍ před onboardingem a alespoň jednou ročně u zpracovatelů, dílčích zpracovatelů, dodavatelů a outsourcovaných poskytovatelů hlášení v rozsahu udržovat v REG08 požadavky na kontakty pro incidenty třetích stran ve finančním sektoru a směrování důkazů.

4.2 Klasifikace a posouzení porušení zabezpečení

4.2.1 [All] Incident Response Coordinator MUSÍ každou položku REG10 do 24 hodin od přijetí klasifikovat jako událost bez PII, podezřelý incident týkající se PII, potvrzený incident týkající se PII, potvrzené porušení zabezpečení osobních údajů, incident týkající se PII ve finančním sektoru, závažný incident ve finančním sektoru, významnou kybernetickou hrozbu nebo položku čekající na klasifikaci.

4.2.2 [Conditional] Information Security Lead MUSÍ v REG10 posoudit dotčené služby, klienty, protistrany, transakce, nedostupnost služeb, geografické rozšíření, ztrátu dat, kritičnost služby a ekonomický dopad, pokud incident týkající se PII může ovlivnit služby nebo operace ve finančním sektoru.

4.2.3 [Both] Privacy Lead / PIMS Manager MUSÍ před finalizací rozhodnutí o oznámení porušení zabezpečení určit dotčenou činnost zpracování, kategorie PII, kategorie subjektů PII, systémy, zpracovatele, dílčí zpracovatele, místa předávání a rizika pro soukromí v REG02, REG04, REG08, REG09 a REG10.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUSÍ u každého potvrzeného nebo důvodně podezřelého porušení zabezpečení osobních údajů posoudit riziko pro dotčené subjekty PII a před přijetím rozhodnutí o externím oznámení zaznamenat doporučení k oznámení, odůvodnění rizika a poradenství v REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUSÍ do 24 hodin po zjištění sdílené odpovědnosti za podezřelé nebo potvrzené porušení zabezpečení osobních údajů zaznamenat rozdělení odpovědnosti společných správců za incident v REG08 a REG10.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUSÍ do 24 hodin poté, co podezřelé nebo potvrzené porušení zabezpečení osobních údajů ovlivní zpracování prováděné jako zpracovatel, posoudit pokyny zákazníka, smluvní oznamovací povinnosti a povinnosti spolupráce v REG08 a REG10.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUSÍ do 24 hodin poté, co podezřelý nebo potvrzený incident týkající se PII ovlivní zpracování prováděné jako dílčí zpracovatel, určit nadřazený oznamovací řetězec a požadované směrování důkazů v REG08 a REG10.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Výjimky

9.1.1 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenat každou výjimku z této politiky v REG12 před implementací, nebo do 24 hodin po nouzovém opatření, pokud předchozí schválení nebylo proveditelné.

9.1.2 [Conditional] Top Management MUSÍ před uzavřením incidentu schválit každou výjimku, která významně ovlivňuje načasování oznámení porušení zabezpečení, načasování hlášení ve finančním sektoru, veřejnou komunikaci, závazek vůči zákazníkovi, uchování důkazů nebo riziko pro subjekt PII, přičemž důkaz o schválení musí být uchován v REG10 a REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ před uzavřením incidentu dokumentovat poradenství ke každému opožděnému oznámení, rozhodnutí o neoznámení, výjimce z hlášení nebo výjimečnému komunikačnímu postupu, přičemž poradenství musí být uchováno v REG10.

9.1.4 [Both] Vendor / Procurement Owner MUSÍ do pěti pracovních dnů po zjištění výjimky zaznamenat výjimky dodavatele, zpracovatele, dílčího zpracovatele, zákazníka nebo outsourcovaného poskytovatele ovlivňující reakci na incidenty ve finančním sektoru v REG08 a REG12.

9.1.5 [All] Privacy Lead / PIMS Manager MUSÍ alespoň měsíčně až do uzavření přezkoumávat otevřené výjimky z této politiky, přičemž stav přezkumu musí být uchován v REG12.

10. Uplatňování politiky

10.1.1 [All] Process Owner / Business Owner MUSÍ do dvou pracovních dnů po zjištění eskalovat selhání při hlášení podezřelého incidentu týkajícího se PII ve finančním sektoru, uchování důkazů, dodržení přidělených opatření nebo spolupráci na posouzení porušení zabezpečení na Privacy Lead / PIMS Manager, přičemž důkazy musí být uchovány v REG12.

10.1.2 [Both] Incident Response Coordinator MUSÍ do jednoho pracovního dne po zjištění problému eskalovat opožděné hlášení, zmeškanou klasifikaci, chybějící důkazy, zmeškanou eskalaci nebo opožděné opatření k zamezení šíření na Privacy Lead / PIMS Manager, přičemž důkazy musí být uchovány v REG10 a REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager MUSÍ zaznamenat neshodu v REG12, pokud porušení této politiky ovlivní příjem incidentu, triáž, zamezení šíření, oznamování, hlášení, integritu důkazů, komunikaci nebo nápravné opatření.

10.1.4 [Both] Vendor / Procurement Owner MUSÍ do pěti pracovních dnů zahájit nápravu dodavatele, zpracovatele, dílčího zpracovatele nebo outsourcovaného poskytovatele prostřednictvím REG08 a REG12, pokud třetí strana nesplní sjednané povinnosti týkající se incidentu, porušení zabezpečení, důkazů nebo hlášení.

10.1.5 [Conditional] Top Management MUSÍ při nejbližším plánovaném přezkoumání vedením přezkoumat významné nebo opakující se neshody s PII15-FS, přičemž rozhodnutí a požadovaná opatření musí být uchována v REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUSÍ do 30 kalendářních dnů aktivovat nápravné školení v REG11, pokud neshoda s politikou zahrnuje povědomí o roli, opožděné hlášení, selhání eskalace, selhání nakládání s důkazy nebo selhání komunikace.

11. Přezkum a údržba

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUSÍ tuto politiku přezkoumat alespoň jednou ročně a zaznamenat výsledek přezkumu, požadované změny a stav schválení v REG12.

11.1.2 [Conditional] Incident Response Coordinator MUSÍ do 30 kalendářních dnů po uzavření každého incidentu s významným dopadem týkajícího se PII ve finančním sektoru, potvrzeného porušení zabezpečení osobních údajů, závažného incidentu ve finančním sektoru nebo významné kybernetické hrozby spustit přezkum této politiky po incidentu, přičemž důkazy o přezkumu musí být uchovány v REG10 a REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUSÍ tuto politiku přezkoumat do 30 kalendářních dnů poté, co se dozví o významné změně právních, odvětvových, zákaznických, smluvních požadavků, požadavků zpracovatele, dílčího zpracovatele, šablony hlášení, lhůty hlášení nebo požadavků na hlášení incidentů souvisejících s předáváním, přičemž důkazy o přezkumu musí být uchovány v REG01, REG08, REG09 a REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUSÍ alespoň jednou ročně přezkoumat implementaci této politiky prostřednictvím programu interního auditu PIMS, přičemž auditní zjištění a nápravná opatření musí být uchována v REG12.

11.1.5 [Conditional] Top Management MUSÍ během plánovaného přezkoumání vedením přezkoumat trendy incidentů, významná porušení zabezpečení, výkonnost hlášení, opožděná nápravná opatření a účinnost politiky, přičemž výstupy musí být uchovány v REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUSÍ alespoň jednou ročně a po každé změně rozsahu PIMS přezkoumat vztah nahrazení mezi PII15-FS a PII15, aby ověřil, že obě politiky nejsou implementovány pro stejný rozsah finančního sektoru, přičemž důkazy o přezkumu musí být uchovány v REG03 a REG12.

12. Související politiky

12.1 Tato politika má být čtena společně s:

12.2 PII01 - Politika systému řízení informací o soukromí

12.3 PII02 - Politika rolí, odpovědností a odpovědnosti v oblasti ochrany soukromí

12.4 PII03 - Politika evidence zpracování PII a právního základu

12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.6 PII06 - Politika řízení práv subjektů PII

12.7 PII07 - Politika posouzení rizik pro soukromí a DPIA

12.8 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení

12.9 PII10 - Politika uchovávání, výmazu a likvidace PII

12.10 PII12 - Politika řízení zpracovatelů, dílčích zpracovatelů a třetích stran v oblasti ochrany soukromí

12.11 PII13 - Politika mezinárodního předávání PII

12.12 PII14 - Politika bezpečnosti PII a řízení přístupu

12.13 PII16 - Politika školení, povědomí a kompetencí v oblasti ochrany soukromí

12.14 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

12.15 PII18 - Politika monitorování, auditu a zlepšování PIMS

12.16 PII23 - Politika cloudového zpracovatele PII, pokud jsou povinnosti cloudového zpracovatele ve finančním sektoru v rozsahu

12.17 PII15 - Politika řízení incidentů PII a porušení zabezpečení PII je základní politikou incidentů a porušení zabezpečení. PII15-FS je náhradní variantou PII15 pro finanční sektor. PII15 a PII15-FS nesmí být implementovány souběžně pro stejný rozsah PIMS, obchodní jednotku, produkt, zákaznické prostředí, regulovanou službu nebo hranici důkazů.

13. Referenční normy a rámce

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].