					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII18					Název dokumentu: **Politika monitorování, auditu a zlepšování PIMS**							
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

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Měření cílů ochrany soukromí
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentované informace k monitorování, auditu a zlepšování
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitorování operativního plánování a řízení
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorování, měření, analýza a vyhodnocování
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Interní audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Přezkoumání vedením
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Neustálé zlepšování
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Neshoda a nápravné opatření
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Záznamy správce o zpracování používané pro audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Důkazy o smlouvě se zpracovatelem a součinnosti při auditu
GDPR	Article 5(2)	Controller	Supporting	Důkazy o odpovědnosti
GDPR	Article 24	Controller	Supporting	Opatření správce a přezkum jejich účinnosti
GDPR	Article 28	Both	Supporting	Správa auditu zpracovatele a součinnosti
GDPR	Article 30	Both	Supporting	Záznamy o zpracování používané pro audit

GDPR	Article 32	Both	Supporting	Testování a hodnocení bezpečnostních opatření
GDPR	Article 39	Conditional	Supporting	Monitorování DPO a poradenství k auditu, je-li relevantní
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Soulad v oblasti soukromí, audit a nezávislý dohled
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Přezkum ochrany PII a kontroly souladu
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitorování a vyhodnocování bezpečnosti informací
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Podpora interního auditu ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Podpora přezkoumání ISMS vedením
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Podpora neustálého zlepšování ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Podpora neshod a nápravných opatření v ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Nezávislý přezkum bezpečnosti informací
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Přezkum souladu politik a norem
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Zásady auditu systému řízení, program, provedení a kompetence

1. Rozsah

1.1 Tato politika stanoví požadavky organizace na monitorování, měření, analýzu, vyhodnocování, interní audit, přezkoumání vedením, řešení neshod, nápravná opatření a neustálé zlepšování PIMS.

1.2 Tato politika se vztahuje na následující oblasti:

1.2.1 všechny procesy, opatření, politiky, registry, důkazní objekty, systémy, dodavatele, zpracovatele, dílčí zpracovatele a ujednání o sdílení údajů v rozsahu PIMS;

1.2.2 kontexty organizace jako správce, společného správce, zpracovatele a dílčího zpracovatele;

1.2.3 konsolidované monitorování výkonnosti PIMS, cílů ochrany soukromí, stavu implementace opatření, zjištění auditu, neshod, nápravných opatření, opatření z přezkoumání vedením a opatření ke zlepšování;

1.2.4 důkazy uchovávané v REG12 a podpůrné zdrojové důkazy uchovávané v REG01 až REG11.

1.3 Tato politika nenahrazuje požadavky na provozní monitorování stanovené v jiných politikách PIMS. Stanoví konsolidovaný cyklus hodnocení výkonnosti, auditu, přezkumu a zlepšování PIMS.

1.4 Pro účely této politiky závažná neshoda PIMS znamená selhání, které podstatně ovlivňuje rozsah PIMS, cíle ochrany soukromí, odpovědnost za zpracování PII, ošetření rizik pro soukromí, práva subjektu PII, zabezpečení zpracování, správu zpracovatele nebo dílčího zpracovatele, připravenost na porušení zabezpečení, integritu dokumentovaných důkazů, rozsah certifikace nebo opakované nesplnění téhož požadavku během období 12 měsíců.

1.5 Pro účely této politiky významná změna znamená jakoukoli změnu ovlivňující rozsah PIMS, účely zpracování PII, kategorie PII, kategorie subjektů PII, místa zpracování, rozdělení rolí správce nebo zpracovatele, architekturu systémů, ujednání s dodavateli nebo dílčími zpracovateli, profil rizik pro soukromí, použitelné právní nebo smluvní povinnosti, rozsah auditu, metodu monitorování nebo rozsah certifikace.

2. Účel

2.1 Účelem této politiky je zajistit, aby organizace hodnotila výkonnost PIMS, ověřovala shodu PIMS, identifikovala neshody, napravovala slabiny opatření a neustále zlepšovala PIMS na základě objektivních důkazů.

2.2 Tato politika umožňuje organizaci doložit, že monitorování PIMS, audity, přezkoumání vedením a činnosti zlepšování jsou plánované, v požadovaných případech nezávislé, založené na důkazech, včasné a dohledatelné ke zodpovědným rolím a kanonickým důkazním objektům.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 definovat konsolidovaný proces monitorování a měření PIMS;

3.1.2 zajistit, aby cíle ochrany soukromí a výkonnost opatření PIMS byly měřeny s využitím dokumentovaných důkazů;

3.1.3 zavést program interního auditu PIMS založený na rizicích;

3.1.4 zachovat nezávislost a objektivitu při auditních činnostech PIMS;

3.1.5 zajistit, aby přezkoumání vedením obdrželo úplné a aktuální vstupy o výkonnosti PIMS;

3.1.6 zajistit, aby neshody byly zaznamenávány, posuzovány, napravovány a ověřovány;

3.1.7 zajistit, aby nápravná opatření byla sledována až do uzavření a přezkoumávána z hlediska účinnosti;

3.1.8 identifikovat opakující se slabiny a příležitosti ke zlepšení;

3.1.9 podporovat připravenost na certifikaci a odpovědnou správu důkazů;

3.1.10 zabránit duplicitě provozních metrik již definovaných v souvisejících politikách PIMS.

4. Prohlášení politiky

4.1 Rámec monitorování a měření PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager musí definovat konsolidovaný program monitorování PIMS v REG12 před zahájením prvního provozu PIMS a poté každoročně.

4.1.2 [Both] Privacy Lead / PIMS Manager musí před zahájením měřicího cyklu definovat v REG12 metodu měření, četnost, zdroj důkazů, cíl a odpovědnou roli pro každou metriku PIMS.

4.1.3 [Both] Process Owner / Business Owner musí čtvrtletně poskytovat Privacy Lead / PIMS Manager vstupy k monitorování činností zpracování PII z REG02.

4.1.4 [Both] Information Security Lead musí čtvrtletně poskytovat Privacy Lead / PIMS Manager vstupy o stavu bezpečnostních opatření pro PII z REG03.

4.1.5 [Both] Vendor / Procurement Owner musí čtvrtletně poskytovat Privacy Lead / PIMS Manager vstupy o stavu zpracovatelů, dílčích zpracovatelů, sdílení se třetími stranami a zajištění dodavatelů z REG08.

4.1.6 [All] Incident Response Coordinator musí měsíčně a do 10 pracovních dnů po uzavření závažného incidentu poskytovat Privacy Lead / PIMS Manager vstupy o trendech incidentů týkajících se soukromí a porušení zabezpečení z REG10.

4.1.7 [Both] Privacy Lead / PIMS Manager musí čtvrtletně konsolidovat výsledky monitorování PIMS v REG12.

4.2 Program interního auditu PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer musí každoročně před prvním plánovaným cyklem auditu PIMS připravit v REG12 program interního auditu PIMS založený na rizicích.

4.2.2 [All] Internal Audit / Compliance Reviewer musí před zahájením auditní práce v terénu definovat v REG12 cíl, kritéria, rozsah, metodu, základ vzorkování a lhůtu pro vykázání každého auditu PIMS.

4.2.3 [All] Internal Audit / Compliance Reviewer musí před každým auditním pověřením zaznamenat v REG12 ověření nezávislosti auditora a střetu zájmů.

4.2.4 [All] Privacy Lead / PIMS Manager musí do 10 pracovních dnů od schválené žádosti o audit zpřístupnit prostřednictvím REG12 vyžádané řízené dokumentované informace PIMS a důkazy z registrů.

4.2.5 [Both] Internal Audit / Compliance Reviewer musí během každého auditu PIMS testovat stav implementace použitelných opatření PIMS proti REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer musí během každého auditu PIMS zaznamenat v REG12 vybraný vzorek důkazů o zpracování PII.

4.2.7 [All] Internal Audit / Compliance Reviewer musí do 15 pracovních dnů po dokončení auditu zaznamenat výsledky auditu PIMS v REG12.

4.2.8 [All] Privacy Lead / PIMS Manager musí do 10 pracovních dnů od přijetí výsledků auditu přiřadit v REG12 vlastníky nápravných opatření pro přijatá zjištění auditu PIMS.

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

9. Výjimky

9.1 Výjimky z monitorování, auditu a zlepšování

9.1.1 [All] Process Owner / Business Owner musí před vznikem odchylky požádat v REG12 o jakoukoli výjimku z této politiky.

9.1.2 [All] Privacy Lead / PIMS Manager musí do 10 pracovních dnů od žádosti posoudit v REG12 dopad každé požadované výjimky na soukromí, certifikaci, audit a nápravná opatření.

9.1.3 [All] Data Protection Officer / Privacy Advisor musí před schválením jakékoli výjimky ovlivňující právní povinnosti, práva subjektu PII, závazky z DPIA, povinnosti zákaznického auditu nebo vysoce rizikové zpracování zaznamenat poradenství v REG12.

9.1.4 [All] Top Management musí před nabytím účinnosti výjimky schválit v REG12 výjimky ovlivňující dokončení harmonogramu auditů, přezkoumání vedením, závažné neshody, rozsah certifikace nebo vysoce rizikové zpracování.

9.1.5 [All] Privacy Lead / PIMS Manager musí pro každou schválenou výjimku z monitorování, auditu nebo zlepšování nastavit v REG12 datum ukončení platnosti nepřesahující 90 dnů.

9.1.6 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od uplynutí platnosti uzavřít nebo znovu posoudit v REG12 každou výjimku z monitorování, auditu nebo zlepšování.

10. Prosazování požadavků

10.1 Prosazování požadavků na monitorování, audit a zlepšování

10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od identifikace zaznamenat v REG12 zmeškaný monitorovací cyklus, zmeškaný audit PIMS, opožděné přezkoumání vedením, chybějící auditní důkazy, opožděné nápravné opatření nebo opožděné opatření ke zlepšení jako neshodu.

10.1.2 [All] Internal Audit / Compliance Reviewer musí před vydáním auditní zprávy zaznamenat v REG12 závažnost zjištění auditu.

10.1.3 [All] Top Management musí do 10 pracovních dnů od eskalace požadovat v REG12 nápravné opatření pro každou závažnou neshodu PIMS.

10.1.4 [All] Process Owner / Business Owner musí před spuštěním do produkčního prostředí nebo předložením externího zajištění zabránit spuštění do produkčního prostředí nebo předložení externího zajištění u vysoce rizikového zpracování, pokud v REG12 chybí požadované důkazy o nápravném opatření.

10.1.5 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů po druhém výskytu během období 12 měsíců eskalovat opakovaně zmeškané lhůty monitorování nebo nápravných opatření na Top Management v REG12.

10.1.6 [All] Internal Audit / Compliance Reviewer musí ověřit uzavření opatření k prosazování požadavků v REG12 při nejbližším plánovaném auditu nebo do 60 dnů od nahlášeného uzavření, podle toho, co nastane dříve.

11. Přezkum a údržba

11.1 Přezkum a údržba politiky

11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat v REG12 každoročně a do 30 dnů od významné změny požadavků na monitorování PIMS, audit, přezkoumání vedením, nápravná opatření nebo certifikaci.

11.1.2 [All] Internal Audit / Compliance Reviewer musí každoročně po posledním plánovaném auditu za provozní rok PIMS přezkoumat v REG12 účinnost programu auditu PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat v REG12 změny této politiky významné z hlediska ochrany soukromí.

11.1.4 [All] Top Management musí před zveřejněním schválit v REG12 významné změny této politiky.

11.1.5 [All] Privacy Lead / PIMS Manager musí do 15 pracovních dnů po schválených změnách této politiky, které mění rozsah PIMS nebo použitelnost opatření, aktualizovat REG01 a REG03.

11.1.6 [All] Privacy Lead / PIMS Manager musí do 30 dnů od zveřejnění zaznamenat v REG11 komunikaci schválených změn této politiky.

12. Související politiky

12.1 Tato politika je podporována následujícími souvisejícími politikami:

12.1.1 PII01 - Politika systému řízení informací o soukromí

12.1.2 PII02 - Politika rolí, odpovědností a odpovědnosti za ochranu soukromí

12.1.3 PII03 - Politika evidence zpracování PII a právního základu

12.1.4 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.1.5 PII05 - Politika správy souhlasů a preferencí

12.1.6 PII06 - Politika správy práv subjektů PII

12.1.7 PII07 - Politika posouzení rizik pro soukromí a DPIA

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

12.1.9 PII09 - Politika shromažďování, používání, zpřístupňování a sdílení PII

12.1.10 PII10 - Politika uchovávání, výmazu a likvidace PII

12.1.11 PII11 - Politika přesnosti a kvality PII

12.1.12 PII12 - Politika řízení ochrany soukromí zpracovatelů, dílčích zpracovatelů a třetích stran

12.1.13 PII13 - Politika mezinárodního předávání PII

12.1.14 PII14 - Politika zabezpečení PII a řízení přístupu

12.1.15 PII15 - Politika řízení incidentů a porušení zabezpečení týkajících se PII

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

12.1.17 PII17 - Politika dokumentovaných informací a správy důkazů PIMS

13. Referenční normy a rámce

13.1 Tato politika je mapována na následující normy a právní předpisy. Mapování vysvětluje, jak politika podporuje citované požadavky, a identifikuje interní ustanovení, která je implementují nebo podporují.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapováno na definování, měření, vykazování a přezkoumávání cílů PIMS a metrik výkonnosti PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapováno na udržování dokumentovaných informací pro výsledky monitorování, programy auditů, výsledky auditů, důkazy pro přezkoumání vedením, neshody, nápravná opatření a opatření ke zlepšování. 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** - Mapováno na provoz plánovaného cyklu monitorování PIMS, auditu, nápravných opatření a zlepšování jako součást operativního řízení PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapováno na definování toho, co je monitorováno a měřeno, konsolidaci výsledků monitorování, hodnocení výkonnosti PIMS a udržování důkazů o měření. 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** - Mapováno na udržování programu interního auditu, plánování auditů, ověření nezávislosti auditora, vzorkování důkazů, výsledky auditů a následná opatření ke zjištěním auditů. 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** - Mapováno na plánování přezkoumání vedením, přezkum výkonnosti PIMS, přezkum trendů auditů a nápravných opatření, schvalování výstupů a rozhodnutí o zdrojích. 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** - Mapováno na identifikaci, schvalování, implementaci a sledování příležitostí k neustálému zlepšování vhodnosti, přiměřenosti a účinnosti PIMS. 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** - Mapováno na zaznamenávání neshod, analýzu kořenové příčiny, plánování nápravných opatření, implementaci nápravných opatření, ověření účinnosti, eskalaci a prosazování požadavků. 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** - Mapováno na záznamy správce o zpracování používané jako zdroje důkazů pro monitorování, auditní vzorkování a metriky aktuálnosti evidence činností zpracování. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapováno na důkazy o smlouvě se zpracovatelem, zákaznickém auditu, odpovědi na zajištění a součinnosti zpracovatele sledované prostřednictvím procesů dodavatelského a zákaznického zajištění. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapováno na důkazy o odpovědnosti pro monitorování, audit, přezkoumání vedením, nápravná opatření a neustálé zlepšování. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapováno na řídicí opatření správce, přezkum účinnosti, přezkoumání vedením, nápravná opatření a dokumentované důkazy o zlepšování. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapováno na důkazy týkající se zpracovatele, dílčího zpracovatele, zákaznického auditu, zajištění třetí stranou a součinnosti dodavatele. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapováno na záznamy o zpracování používané jako důkazy pro monitorování, auditní vzorkování, úplnost důkazních objektů a aktuálnost evidence činností zpracování. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapováno na monitorování a hodnocení stavu bezpečnostních opatření pro PII, důkazy o technických opatřeních a důkazy o účinnosti související s bezpečností. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapováno na poradenství v oblasti ochrany soukromí, poznatky z monitorování, podporu auditů a přezkum trendů souladu v oblasti ochrany soukromí prováděný Data Protection Officer / Privacy Advisor, je-li relevantní. 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** - Mapováno na ověřování souladu v oblasti ochrany soukromí, interní nebo nezávislé audity, interní opatření, mechanismy dohledu a důkazy z posouzení rizik pro soukromí. 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** - Mapováno na nezávislý přezkum informační bezpečnosti související s PII, soulad s politikami a normami a technický přezkum souladu při ochraně PII. 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** - Mapováno na vstupy z monitorování a hodnocení bezpečnosti informací, které podporují měření výkonnosti PIMS a stavu bezpečnostních opatření pro PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapováno na podporu interního auditu ISMS pro plánování auditu PIMS, auditní důkazy, výsledky auditu a dokončení programu auditu. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapováno na vstupy a výstupy přezkoumání vedením pro integrovaný dohled nad výkonností PIMS a bezpečnosti informací. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapováno na neustálé zlepšování PIMS a podpůrného prostředí opatření bezpečnosti informací. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapováno na řešení neshod, plánování nápravných opatření, implementaci nápravných opatření a ověření účinnosti. 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 - Mapováno na nezávislý přezkum, ověření nezávislosti auditora, testování auditních důkazů a nezávislé ověření účinnosti nápravných opatření. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapováno na přezkum souladu PIMS a politik bezpečnosti informací, stavu implementace opatření a důkazů o shodě s normami. 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** - Mapováno na zásady auditu, řízení programu auditů, provádění auditů, auditní vykazování založené na důkazech, následná auditní opatření a očekávání kompetencí auditorů pro audity PIMS. 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].