					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII14					Název dokumentu: **Politika zabezpečení PII a řízení přístupu**							
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 6.1.3; Clause 8.1	Both	Primary	Plánování a provoz bezpečnostních opatření pro PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Důkazy, monitorování a nápravná opatření
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identita a přístupová práva pro zpracování PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Ochrana koncových bodů a silná autentizace
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Protokolování a kryptografická ochrana
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Zabezpečení aplikací a bezpečná architektura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Ochrana a přezkum záznamů
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Bezpečnost, odpovědnost a opatření zpracovatele
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integrace opatření ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Pokyny k implementaci bezpečnostních opatření
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zásady bezpečnosti informací a souladu v oblasti ochrany soukromí

ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Bezpečnostní opatření pro ochranu PII

1. Rozsah

1.1 Tato politika stanoví požadavky na zabezpečení a řízení přístupu specifické pro PII pro systémy, aplikace, služby, zařízení, cloudová prostředí a provozní procesy, které PII ukládají, přenášejí, zpracovávají, zpřístupňují, spravují nebo chrání.

1.2 Tato politika se vztahuje na kontexty správce, společného správce, zpracovatele a dílčího zpracovatele, ve kterých organizace určuje, provozuje, podporuje nebo využívá bezpečnostní opatření pro zpracování PII.

1.3 Tato politika pokrývá následující domény bezpečnostních kontrol PII:

1.3.1 základní soubor bezpečnostních opatření pro PII a integraci se stávajícími politikami bezpečnosti informací;

1.3.2 řízení přístupu;

1.3.3 autentizaci;

1.3.4 privilegovaný přístup;

1.3.5 šifrování a bezpečné ukládání;

1.3.6 protokolování a monitorování;

1.3.7 bezpečnou konfiguraci a řízení zranitelností;

1.3.8 opatření pro přístup z koncových bodů a cloudu;

1.3.9 vazbu důkazů prostřednictvím REG02, REG08, REG10 a REG12.

1.4 Tato politika nenahrazuje úplný systém řízení bezpečnosti informací, politiku zabezpečení sítí, politiku bezpečného vývoje, politiku zálohování, politiku koncových bodů, politiku zabezpečení cloudu, kryptografický standard, postup řízení zranitelností ani postup reakce na incidenty. Pokud již takové politiky existují, tato politika stanoví vazby a požadavky na důkazy specifické pro PII potřebné pro zajištění PIMS.

1.5 Tato politika neduplikuje:

1.5.1 evidenci činností zpracování PII a vlastnictví právního základu v PII03;

1.5.2 metodiku posouzení rizik pro soukromí a DPIA v PII07;

1.5.3 kontrolní brány ochrany soukromí již od návrhu v PII08;

1.5.4 pravidla pro shromažďování, použití, zpřístupnění a sdílení v PII09;

1.5.5 provádění uchovávání, výmazu a likvidace v PII10;

1.5.6 správu životního cyklu zpracovatelů v PII12;

1.5.7 opatření mechanismů mezinárodního předávání v PII13;

1.5.8 pracovní postup pro incidenty a porušení zabezpečení v PII15;

1.5.9 správu dokumentovaných informací v PII17;

1.5.10 správu monitorování, auditu a zlepšování PIMS v PII18.

1.6 Pro účely této politiky jsou provozní logy, výstupy bezpečnostních nástrojů, exporty přezkumů přístupových práv, zprávy o zranitelnostech a důkazy o konfiguraci zdroji důkazů, které se přikládají ke kanonickým důkazním objektům, shrnují se v nich nebo se na ně odkazuje. Nejsou samostatnými registry PIMS.

2. Účel

2.1 Účelem této politiky je zajistit, aby PII byly v průběhu zpracování chráněny vhodnými, rizikově přiměřenými a auditovatelnými bezpečnostními opatřeními a opatřeními řízení přístupu.

2.2 Tato politika umožňuje organizaci prokázat, že bezpečnostní opatření pro PII jsou plánována, implementována, přezkoumávána, monitorována a zlepšována prostřednictvím REG02, REG08,

REG10 a REG12, aniž by vznikaly duplicitní bezpečnostní registry nebo docházelo k nahrazení stávajících politik bezpečnosti informací.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 stanovit základní požadavky na řízení přístupu k PII pro systémy a činnosti zpracování;

3.1.2 zajistit, aby opatření autentizace odpovídala citlivosti PII a kontextu přístupu;

3.1.3 stanovit požadavky na přezkum privilegovaného i běžného přístupu k PII;

3.1.4 stanovit očekávání týkající se šifrování a bezpečného ukládání PII v klidu, při přenosu a v relevantních cloudových nebo koncových kontextech;

3.1.5 stanovit očekávání týkající se protokolování a monitorování přístupu k PII, změn PII a správy PII;

3.1.6 stanovit požadavky na důkazy o bezpečné konfiguraci a zranitelnostech pro systémy zpracovávající PII;

3.1.7 stanovit očekávání týkající se přístupu z koncových bodů a cloudu, aniž by vznikala úplná politika koncových bodů nebo zabezpečení cloudu;

3.1.8 propojit podezření na bezpečnostní incidenty týkající se PII s REG10 bez duplikace pracovního postupu pro incidenty;

3.1.9 integrovat tuto politiku se stávajícími politikami bezpečnosti informací, pokud jsou k dispozici;

3.1.10 udržovat důkazy připravené pro audit výhradně pomocí REG02, REG08, REG10 a REG12.

4. Prohlášení politiky

4.1 Základní soubor bezpečnostních opatření pro PII a integrace s ISMS

4.1.1 [Both] Information Security Lead MUSÍ před uvedením systému nebo služby do produkčního prostředí nebo před významnou změnou definovat v REG12 základní soubor bezpečnostních opatření pro PII pro každý systém nebo službu, které zpracovávají PII.

4.1.2 [Both] System Owner / Application Owner MUSÍ před spoléháním se na existující opatření bezpečnosti informací pro účely zajištění PIMS zaznamenat v REG12 umístění důkazů o bezpečnostních opatřeních pro PII.

4.1.3 [Controller] Process Owner / Business Owner MUSÍ před požadavkem na nový nebo významně změněný přístup k PII identifikovat v REG02 citlivost PII, kontext zpracování a potřebu přístupu.

4.1.4 [Processor] Vendor / Procurement Owner MUSÍ před zahájením nebo významnou změnou přístupu zpracovatele k PII zákazníka zaznamenat v REG08 bezpečnostní pokyny zákazníka, hranice odpovědnosti zákazníka a bezpečnostní závazky zpracovatele.

4.1.5 [Both] Privacy Lead / PIMS Manager MUSÍ před přijetím činnosti zpracování jako auditovatelné v rámci PIMS ověřit, že důkazy o zabezpečení PII jsou propojeny s REG02, REG08, REG10 nebo REG12.

4.2 Základní požadavky na řízení přístupu

4.2.1 [Both] System Owner / Application Owner MUSÍ před povolením přístupu omezit přístup k PII na schválené role a oprávněné uživatele zaznamenané nebo dohledatelné v REG02 nebo REG12.

4.2.2 [Both] Process Owner / Business Owner MUSÍ před zřízením přístupu ze strany System Owner / Application Owner schválit obchodní účel přístupu k PII v REG02 nebo REG12.

4.2.3 [Both] System Owner / Application Owner MUSÍ alespoň čtvrtletně přezkoumat uživatelský přístup k systémům zpracovávajícím PII s vysokým dopadem nebo citlivé PII a zaznamenat výsledek přezkumu v REG12.

4.2.4 [Both] System Owner / Application Owner MUSÍ alespoň jednou ročně přezkoumat uživatelský přístup k ostatním systémům zpracovávajícím PII a zaznamenat výsledek přezkumu v REG12.

4.2.5 [Both] System Owner / Application Owner MUSÍ do jednoho pracovního dne po změně role, ukončení, dokončení smlouvy nebo poté, co přístup již není vyžadován, odebrat nebo změnit přístup k PII v REG12.

4.2.6 [Processor] Vendor / Procurement Owner MUSÍ před povolením nebo změnou přístupu potvrdit v REG08, že přístup zpracovatele k PII zákazníka je omezen na dokumentované pokyny zákazníka.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUSÍ před povolením nebo změnou přístupu dílčího zpracovatele potvrdit v REG08, že přístup dílčího zpracovatele k PII je omezen na oprávněné činnosti dílčího zpracování.

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

9. Výjimky

9.1.1 [Both] Information Security Lead MUSÍ před aktivací výjimky zaznamenat v REG12 každou výjimku z požadavku na zabezpečení PII nebo řízení přístupu.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUSÍ před schválením poskytnout poradenství k bezpečnostním výjimkám týkajícím se PII s vyšším rizikem v REG12.

9.1.3 [Both] Top Management MUSÍ před aktivací schválit v REG12 bezpečnostní výjimky týkající se PII, pokud výjimka ovlivňuje PII s vysokým dopadem, citlivé PII, privilegovaný přístup, šifrování, protokolování nebo nevyřešené vysoce rizikové zranitelnosti.

9.1.4 [Both] Information Security Lead MUSÍ před schválením výjimky definovat v REG12 datum skončení platnosti výjimky, kompenzační opatření a datum přezkumu.

9.1.5 [Both] System Owner / Application Owner MUSÍ do pěti pracovních dnů po skončení platnosti napravit, obnovit nebo uzavřít expirované bezpečnostní výjimky týkající se PII v REG12.

9.1.6 [Processor] Vendor / Procurement Owner MUSÍ před přijetím zaznamenat v REG08 a REG12 bezpečnostní výjimky zpracovatele nebo dílčího zpracovatele ovlivňující PII zákazníka.

10. Prosazování požadavků politiky

10.1.1 [Both] Privacy Lead / PIMS Manager MUSÍ do pěti pracovních dnů od identifikace zaznamenat v REG12 neshody týkající se chybějících nebo neúplných důkazů o zabezpečení PII.

10.1.2 [Both] Information Security Lead MUSÍ do pěti pracovních dnů od validace přiřadit v REG12 vlastnictví nápravy selhání bezpečnostních opatření pro PII.

10.1.3 [Both] System Owner / Application Owner MUSÍ do jednoho pracovního dne od validace zakázat nebo omezit neoprávněný, nadměrný nebo nepodložený přístup k PII a zaznamenat toto opatření v REG12.

10.1.4 [Conditional] Incident Response Coordinator MUSÍ do jednoho pracovního dne propojit prosazovací opatření s REG10, pokud se věc prosazování týká podezřelého nebo potvrzeného incidentu týkajícího se PII.

10.1.5 [Both] Top Management MUSÍ před přezkoumáním vedením přezkoumat v REG12 opakované nebo vysoce rizikové neshody v oblasti zabezpečení PII.

11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager MUSÍ alespoň jednou ročně přezkoumat tuto politiku společně s Information Security Lead a zaznamenat výsledek přezkumu v REG12.

11.1.2 [Both] Information Security Lead MUSÍ do 30 dnů po významné technologické změně, změně hrozeb, auditu, incidentu nebo regulační změně ovlivňující zabezpečení PII přezkoumat v REG12 základní soubor bezpečnostních opatření pro PII.

11.1.3 [Both] System Owner / Application Owner MUSÍ do 30 dnů po významné změně architektury, přístupu, konfigurace, zranitelnosti nebo protokolování aktualizovat v REG12 důkazy o zabezpečení PII na úrovni systému.

11.1.4 [Processor] Vendor / Procurement Owner MUSÍ do 30 dnů po významné změně služby, pokynu zákazníka nebo dílčího zpracovatele přezkoumat v REG08 důkazy o bezpečnostních odpovědnostech zpracovatele a dílčího zpracovatele týkajících se PII.

11.1.5 [All] Internal Audit / Compliance Reviewer MUSÍ podle schváleného plánu auditů ověřit důkazy o přezkumu politiky a vybrané důkazy o bezpečnostních opatřeních pro PII v REG12.

12. Související politiky

12.1 Tato politika by měla být čtena společně s:

12.1.1 PII01 - Politika systému řízení informací o soukromí;

12.1.2 PII02 - Politika rolí, odpovědností a odpovědnosti v oblasti soukromí;

12.1.3 PII03 - Politika evidence zpracování PII a právního základu;

12.1.4 PII07 - Politika posouzení rizik pro soukromí a DPIA;

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

12.1.6 PII09 - Politika shromažďování, použití, zpřístupnění a sdílení PII;

12.1.7 PII10 - Politika uchovávání, výmazu a likvidace PII;

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

12.1.9 PII13 - Politika mezinárodního předávání PII;

12.1.10 PII15 - Politika řízení incidentů a porušení zabezpečení týkajících se PII;

12.1.11 PII16 - Politika školení, povědomí a kompetencí v oblasti soukromí;

12.1.12 PII17 - Politika správy dokumentovaných informací a důkazů PIMS;

12.1.13 PII18 - Politika monitorování, auditu a zlepšování PIMS.

13. Referenční normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].