					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII14					Názov dokumentu: **Politika bezpečnosti PII a riadenia prístupu**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma / predpis	Kapitola / kontrola / článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Plánovanie a prevádzka bezpečnostných kontrol PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Dôkazy, monitorovanie a nápravné opatrenia
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identita a prístupové práva pri spracúvaní PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Ochrana koncových bodov a bezpečná autentifikácia
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logovanie a kryptografická ochrana
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Bezpečnosť aplikácií a bezpečná architektúra
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Ochrana a preskúmanie záznamov
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Bezpečnosť, preukázateľná zodpovednosť a kontroly sprostredkovateľa
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	Integrácia kontrol 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	Usmernenie k implementácii bezpečnostných kontrol
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Princípy informačnej bezpečnosti a súladu v oblasti ochrany súkromia

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	Bezpečnostné kontroly ochrany PII

1. Rozsah

1.1 Táto politika stanovuje požiadavky na bezpečnosť a riadenie prístupu špecifické pre PII pre systémy, aplikácie, služby, zariadenia, cloudové prostredia a prevádzkové procesy, ktoré PII uchovávajú, prenášajú, spracúvajú, sprístupňujú, spravujú alebo chránia.

1.2 Táto politika sa uplatňuje v kontextoch prevádzkovateľa, spoločného prevádzkovateľa, sprostredkovateľa a ďalšieho sprostredkovateľa, v ktorých organizácia určuje, prevádzkuje, podporuje alebo využíva bezpečnostné kontroly na spracúvanie PII.

1.3 Táto politika pokrýva tieto oblasti bezpečnostných opatrení pre PII:

1.3.1 referenčnú úroveň bezpečnosti PII a integráciu s existujúcimi politikami informačnej bezpečnosti;

1.3.2 riadenie prístupu;

1.3.3 autentifikáciu;

1.3.4 privilegovaný prístup;

1.3.5 šifrovanie a bezpečné úložisko;

1.3.6 logovanie a monitorovanie;

1.3.7 bezpečnú konfiguráciu a riadenie zraniteľností;

1.3.8 kontroly prístupu z koncových bodov a v cloude;

1.3.9 väzbu dôkazov prostredníctvom REG02, REG08, REG10 a REG12.

1.4 Táto politika nenahrádza úplný systém manažérstva informačnej bezpečnosti, politiku bezpečnosti sietí, politiku bezpečného vývoja, politiku zálohovania, politiku koncových bodov, politiku cloudovej bezpečnosti, kryptografický štandard, postup riadenia zraniteľností ani postup reakcie na incidenty. Ak takéto politiky už existujú, táto politika stanovuje väzby a požiadavky na dôkazy špecifické pre PII, ktoré sú potrebné na uistenie v rámci PIMS.

1.5 Táto politika neduplikuje:

1.5.1 evidenciu spracúvania PII a vlastníctvo právneho základu v PII03;

1.5.2 metodiku posúdenia rizík ochrany súkromia a DPIA v PII07;

1.5.3 kontrolné brány ochrany súkromia už od návrhu v PII08;

1.5.4 pravidlá zberu, používania, poskytovania a zdieľania v PII09;

1.5.5 vykonávanie uchovávania, výmazu a likvidácie v PII10;

1.5.6 správu životného cyklu sprostredkovateľa v PII12;

1.5.7 kontroly mechanizmov medzinárodného prenosu v PII13;

1.5.8 pracovný tok incidentov a porušení ochrany údajov v PII15;

1.5.9 správu zdokumentovaných informácií v PII17;

1.5.10 správu monitorovania, auditu a zlepšovania PIMS v PII18.

1.6 Na účely tejto politiky sú prevádzkové logy, výstupy bezpečnostných nástrojov, exporty revízií prístupových práv, správy o zraniteľnostiach a konfiguračné dôkazy zdrojmi dôkazov, ktoré sa pripájajú ku kanonickým dôkazovým objektom, sumarizujú sa v nich alebo sa na ne v nich odkazuje. Nie sú samostatnými registrami PIMS.

2. Účel

2.1 Účelom tejto politiky je zabezpečiť, aby boli PII počas celého spracúvania chránené primeranými, rizikovo zosúladenými a auditovateľnými bezpečnostnými a prístupovými kontrolami.

2.2 Táto politika umožňuje organizácii preukázať, že bezpečnostné kontroly PII sú plánované, implementované, preskúmavané, monitorované a zlepšované prostredníctvom REG02, REG08,

REG10 a REG12 bez vytvárania duplicitných bezpečnostných registrov alebo nahrádzania existujúcich politík informačnej bezpečnosti.

3. Ciele

3.1 Cieľmi tejto politiky je:

3.1.1 definovať základ riadenia prístupu k PII pre systémy a spracovateľské činnosti;

3.1.2 zabezpečiť, aby autentifikačné kontroly zodpovedali citlivosti PII a kontextu prístupu k nim;

3.1.3 definovať požiadavky na preskúmanie privilegovaného a bežného prístupu k PII;

3.1.4 definovať očakávania týkajúce sa šifrovania a bezpečného úložiska pre PII v pokoji, pri prenose a v relevantných cloudových alebo endpointových kontextoch;

3.1.5 definovať očakávania týkajúce sa logovania a monitorovania prístupu k PII, zmien PII a správy PII;

3.1.6 definovať požiadavky na dôkazy o bezpečnej konfigurácii a zraniteľnostiach systémov spracúvajúcich PII;

3.1.7 definovať očakávania týkajúce sa prístupu z koncových bodov a v cloude bez vytvorenia úplnej politiky koncových bodov alebo cloudovej bezpečnosti;

3.1.8 prepojiť podozrenia na bezpečnostné incidenty PII s REG10 bez duplikovania pracovného toku incidentov;

3.1.9 integrovať sa s existujúcimi politikami informačnej bezpečnosti, ak sú k dispozícii;

3.1.10 udržiavať dôkazy pripravené na audit výlučne prostredníctvom REG02, REG08, REG10 a REG12.

4. Vyhlásenia politiky

4.1 Referenčná úroveň bezpečnosti PII a integrácia s ISMS

4.1.1 [Both] Information Security Lead MUST definovať referenčnú úroveň bezpečnosti PII pre každý systém alebo službu, ktorá spracúva PII, v REG12 pred uvedením systému alebo služby do produkčného prostredia alebo pred podstatnou zmenou.

4.1.2 [Both] System Owner / Application Owner MUST zaznamenať umiestnenie dôkazov o implementovaných bezpečnostných kontrolách PII v REG12 pred tým, ako sa existujúca kontrola informačnej bezpečnosti použije na uistenie v rámci PIMS.

4.1.3 [Controller] Process Owner / Business Owner MUST identifikovať citlivosť PII, kontext spracúvania a potrebu prístupu v REG02 pred vyžiadaním nového alebo podstatne zmeneného prístupu k PII.

4.1.4 [Processor] Vendor / Procurement Owner MUST zaznamenať bezpečnostné pokyny zákazníka, hranice zodpovedností zákazníka a bezpečnostné záväzky sprostredkovateľa v REG08 pred začiatkom prístupu sprostredkovateľa k PII zákazníka alebo pred jeho podstatnou zmenou.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST overiť, že dôkazy o bezpečnosti PII sú prepojené s REG02, REG08, REG10 alebo REG12 pred prijatím spracovateľskej činnosti ako auditovateľnej v rámci PIMS.

4.2 Základ riadenia prístupu

4.2.1 [Both] System Owner / Application Owner MUST obmedziť prístup k PII na schválené roly a oprávnených používateľov zaznamenaných alebo sledovateľných v REG02 alebo REG12 pred povolením prístupu.

4.2.2 [Both] Process Owner / Business Owner MUST schváliť obchodný účel prístupu k PII v REG02 alebo REG12 pred tým, ako System Owner / Application Owner zriadi prístup.

4.2.3 [Both] System Owner / Application Owner MUST preskúmať prístup používateľov k systémom spracúvajúcim PII s vysokým dopadom alebo citlivé PII najmenej štvrťročne a zaznamenať výsledok preskúmania v REG12.

4.2.4 [Both] System Owner / Application Owner MUST preskúmať prístup používateľov k ostatným systémom spracúvajúcim PII najmenej raz ročne a zaznamenať výsledok preskúmania v REG12.

4.2.5 [Both] System Owner / Application Owner MUST odstrániť alebo upraviť prístup k PII v REG12 do jedného pracovného dňa po zmene roly, ukončení pracovného alebo zmluvného vzťahu, dokončení zmluvy alebo ak prístup už nie je potrebný.

4.2.6 [Processor] Vendor / Procurement Owner MUST potvrdiť v REG08, že prístup sprostredkovateľa k PII zákazníka je obmedzený na zdokumentované pokyny zákazníka, pred povolením alebo zmenou prístupu.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST potvrdiť v REG08, že prístup ďalšieho sprostredkovateľa k PII je obmedzený na autorizované činnosti ďalšieho sprostredkovania, pred povolením alebo zmenou prístupu ďalšieho sprostredkovateľa.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Výnimky

9.1.1 [Both] Information Security Lead MUST zaznamenať každú výnimku z požiadavky na bezpečnosť PII alebo riadenie prístupu v REG12 pred aktiváciou výnimky.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST poskytnúť stanovisko k vyššie rizikovým bezpečnostným výnimkám PII v REG12 pred schválením.

9.1.3 [Both] Top Management MUST schváliť bezpečnostné výnimky PII v REG12 pred aktiváciou, ak výnimka ovplyvňuje PII s vysokým dopadom, citlivé PII, privilegovaný prístup, šifrovanie, logovanie alebo nevyriešené vysoko rizikové zraniteľnosti.

9.1.4 [Both] Information Security Lead MUST definovať skončenie platnosti výnimky, kompenzačnú kontrolu a dátum preskúmania v REG12 pred schválením výnimky.

9.1.5 [Both] System Owner / Application Owner MUST napraviť, obnoviť alebo uzavrieť bezpečnostné výnimky PII po uplynutí platnosti v REG12 do piatich pracovných dní po uplynutí platnosti.

9.1.6 [Processor] Vendor / Procurement Owner MUST zaznamenať bezpečnostné výnimky sprostredkovateľa alebo ďalšieho sprostredkovateľa ovplyvňujúce PII zákazníka v REG08 a REG12 pred akceptáciou.

10. Uplatňovanie politiky

10.1.1 [Both] Privacy Lead / PIMS Manager MUST zaznamenať nezhody pre chýbajúce alebo neúplné bezpečnostné dôkazy PII v REG12 do piatich pracovných dní od identifikácie.

10.1.2 [Both] Information Security Lead MUST priradiť vlastníctvo nápravy pri zlyhaniach bezpečnostných kontrol PII v REG12 do piatich pracovných dní od validácie.

10.1.3 [Both] System Owner / Application Owner MUST zakázať alebo obmedziť neoprávnený, nadmerný alebo nepodložený prístup k PII do jedného pracovného dňa od validácie a zaznamenať opatrenie v REG12.

10.1.4 [Conditional] Incident Response Coordinator MUST prepojiť opatrenia uplatňovania politiky s REG10 do jedného pracovného dňa, keď sa záležitosť uplatňovania politiky týka podozrivého alebo potvrdeného incidentu PII.

10.1.5 [Both] Top Management MUST preskúmať opakované alebo vysoko rizikové bezpečnostné nezhody PII v REG12 pred preskúmaním manažmentom.

11. Preskúmanie a údržba

11.1.1 [All] Privacy Lead / PIMS Manager MUST preskúmať túto politiku s Information Security Lead najmenej raz ročne a zaznamenať výsledok preskúmania v REG12.

11.1.2 [Both] Information Security Lead MUST preskúmať referenčnú úroveň bezpečnosti PII v REG12 do 30 dní po podstatnej technologickej zmene, zmene hrozieb, audite, incidente alebo regulačnej zmene ovplyvňujúcej bezpečnosť PII.

11.1.3 [Both] System Owner / Application Owner MUST aktualizovať dôkazy o bezpečnosti PII na úrovni systému v REG12 do 30 dní po podstatnej zmene architektúry, prístupu, konfigurácie, zraniteľnosti alebo logovania.

11.1.4 [Processor] Vendor / Procurement Owner MUST preskúmať dôkazy o bezpečnostných zodpovednostiach sprostredkovateľa a ďalšieho sprostredkovateľa pri PII v REG08 do 30 dní po podstatnej zmene služby, pokynu zákazníka alebo ďalšieho sprostredkovateľa.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST overiť dôkazy o preskúmaní politiky a vybrané dôkazy o bezpečnostných kontrolách PII v REG12 podľa schváleného plánu auditov.

12. Súvisiace politiky

12.1 Táto politika sa má čítať spolu s:

12.2 PII01 - Politika systému manažérstva ochrany súkromia;

12.3 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia;

12.4 PII03 - Politika evidencie spracúvania PII a právneho základu;

12.5 PII07 - Politika posúdenia rizík ochrany súkromia a DPIA;

12.6 PII08 - Politika ochrany súkromia už od návrhu a štandardne;

12.7 PII09 - Politika zberu, používania, poskytovania a zdieľania PII;

12.8 PII10 - Politika uchovávania, výmazu a likvidácie PII;

12.9 PII12 - Politika riadenia ochrany súkromia u sprostredkovateľov, ďalších sprostredkovateľov a tretích strán;

12.10 PII13 - Politika medzinárodného prenosu PII;

12.11 PII15 - Politika riadenia incidentov a porušení ochrany PII;

12.12 PII16 - Politika školenia, povedomia a kompetentnosti v oblasti ochrany súkromia;

12.13 PII17 - Politika zdokumentovaných informácií PIMS a riadenia dôkazov;

12.14 PII18 - Politika monitorovania, auditu a zlepšovania PIMS.

13. Referenčné 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].