					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: PII14					Naslov dokumenta: **Politika varnosti PII in nadzora dostopa**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/kontrola/člen	Uporabljivost	Vrsta pokritja	Komentar
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Načrtovanje in izvajanje varnostnih kontrol za PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Dokazila, spremljanje in korektivni ukrepi
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitete in pravice dostopa za obdelavo PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Zaščita končnih točk in varna avtentikacija
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Beleženje in kriptografska zaščita
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Varnost aplikacij in varna arhitektura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Zaščita in pregled zapisov
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Varnost, odgovornost in kontrole obdelovalcev
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	Integracija 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	Smernice za implementacijo varnostnih kontrol
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načeli informacijske varnosti in skladnosti zasebnosti
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;	Both	Supporting	Varnostne kontrole za zaščito PII

	Clause 18.2.3; Clause 18.2.4			

1. Področje uporabe

1.1 Ta politika določa posebne zahteve glede varnosti in nadzora dostopa za PII za sisteme, aplikacije, storitve, naprave, okolja v oblaku in operativne procese, ki hranijo, prenašajo, obdelujejo, dostopajo do, upravljajo ali varujejo PII.

1.2 Ta politika se uporablja za okoliščine upravljavca, skupnega upravljavca, obdelovalca in podobdelovalca, kadar organizacija določa, izvaja, podpira ali se zanaša na varnostne kontrole za obdelavo PII.

1.3 Ta politika zajema naslednja področja varnostnih kontrol za PII:

1.3.1 osnovni nabor varnostnih zahtev za PII in integracijo z obstoječimi politikami informacijske varnosti;

1.3.2 nadzor dostopa;

1.3.3 avtentikacijo;

1.3.4 privilegirani dostop;

1.3.5 šifriranje in varno hrambo;

1.3.6 beleženje in spremljanje;

1.3.7 varno konfiguracijo in upravljanje ranljivosti;

1.3.8 kontrole dostopa do končnih točk in oblaka;

1.3.9 povezavo z dokazili prek REG02, REG08, REG10 in REG12.

1.4 Ta politika ne nadomešča celovitega sistema upravljanja informacijske varnosti, politike varnosti omrežja, politike varnega razvoja, politike varnostnega kopiranja, politike končnih točk, politike varnosti v oblaku, kriptografskega standarda, postopka upravljanja ranljivosti ali postopka odzivanja na incidente. Kadar take politike že obstajajo, ta politika določa posebne povezave in zahteve glede dokazil za PII, potrebne za zagotavljanje PIMS.

1.5 Ta politika ne podvaja:

1.5.1 lastništva popisa dejavnosti obdelave PII in pravne podlage v PII03;

1.5.2 metodologije tveganj za zasebnost in DPIA v PII07;

1.5.3 kontrolnih točk varstva zasebnosti že pri načrtovanju v PII08;

1.5.4 pravil zbiranja, uporabe, razkritja in deljenja v PII09;

1.5.5 izvajanja hrambe, izbrisa in odstranjevanja v PII10;

1.5.6 upravljanja življenjskega cikla obdelovalcev v PII12;

1.5.7 kontrol mehanizmov mednarodnega prenosa v PII13;

1.5.8 delovnega toka za incidente in kršitve v PII15;

1.5.9 upravljanja dokumentiranih informacij v PII17;

1.5.10 upravljanja spremljanja, presoje in izboljševanja PIMS v PII18.

1.6 Za namene te politike so operativni dnevniki, izhodi varnostnih orodij, izvozi pregledov pravic dostopa, poročila o ranljivostih in konfiguracijska dokazila viri dokazil, ki se priložijo kanoničnim dokazilnim objektom, se v njih povzamejo ali se nanje sklicujejo. Niso ločeni registri PIMS.

2. Namen

2.1 Namen te politike je zagotoviti, da so PII med celotno obdelavo zaščiteni z ustreznimi, s tveganji usklajenimi in revizijsko preverljivimi varnostnimi kontrolami ter kontrolami dostopa.

2.2 Ta politika organizaciji omogoča dokazovanje, da so varnostne kontrole za PII načrtovane, implementirane, pregledovane, spremljane in izboljševane prek REG02, REG08, REG10 in REG12, brez vzpostavljanja podvojenih varnostnih registrov ali nadomeščanja obstoječih politik informacijske varnosti.

3. Cilji

3.1 Cilji te politike so:

3.1.1 določiti osnovni nabor kontrol dostopa do PII za sisteme in dejavnosti obdelave;

3.1.2 zagotoviti, da so avtentikacijske kontrole ustrezne glede na občutljivost PII in kontekst dostopa;

3.1.3 določiti zahteve za pregled privilegiranega in običajnega dostopa do PII;

3.1.4 določiti pričakovanja glede šifriranja in varne hrambe PII v mirovanju, med prenosom ter v relevantnih okoljih oblaka ali končnih točk;

3.1.5 določiti pričakovanja glede beleženja in spremljanja dostopa do PII, sprememb PII in upravljanja PII;

3.1.6 določiti zahteve glede dokazil o varni konfiguraciji in ranljivostih za sisteme, ki obdelujejo PII;

3.1.7 določiti pričakovanja glede dostopa prek končnih točk in oblaka, brez vzpostavitve celovite politike končnih točk ali varnosti v oblaku;

3.1.8 povezati domnevne varnostne incidente v zvezi s PII z REG10, brez podvajanja delovnega toka za incidente;

3.1.9 se povezati z obstoječimi politikami informacijske varnosti, kadar so na voljo;

3.1.10 vzdrževati dokazila, pripravljena za revizijo, z uporabo samo REG02, REG08, REG10 in REG12.

4. Določbe politike

4.1 Osnovni nabor varnostnih zahtev za PII in integracija z ISMS

4.1.1 [Both] Information Security Lead mora določiti osnovni nabor varnostnih zahtev za PII za vsak sistem ali storitev, ki obdeluje PII, v REG12, preden sistem ali storitev preide v produkcijo ali se bistveno spremeni.

4.1.2 [Both] System Owner / Application Owner mora v REG12 evidentirati lokacijo dokazil o implementiranih varnostnih kontrolah za PII, preden se za zagotavljanje PIMS zanaša na obstoječo kontrolo informacijske varnosti.

4.1.3 [Controller] Process Owner / Business Owner mora v REG02 opredeliti občutljivost PII, kontekst obdelave in potrebo po dostopu, preden zahteva nov ali bistveno spremenjen dostop do PII.

4.1.4 [Processor] Vendor / Procurement Owner mora v REG08 evidentirati varnostna navodila naročnika, meje odgovornosti naročnika in varnostne zaveze obdelovalca, preden se začne ali bistveno spremeni dostop obdelovalca do PII naročnika.

4.1.5 [Both] Privacy Lead / PIMS Manager mora preveriti, da so dokazila o varnosti PII povezana z REG02, REG08, REG10 ali REG12, preden dejavnost obdelave sprejme kot primerno za presojo PIMS.

4.2 Osnovni nabor kontrol dostopa

4.2.1 [Both] System Owner / Application Owner mora omejiti dostop do PII na odobrene vloge in pooblaščene uporabnike, evidentirane ali sledljive v REG02 ali REG12, preden se dostop omogoči.

4.2.2 [Both] Process Owner / Business Owner mora odobriti poslovni namen dostopa do PII v REG02 ali REG12, preden System Owner / Application Owner dodeli dostop.

4.2.3 [Both] System Owner / Application Owner mora najmanj četrtletno pregledati uporabniški dostop do sistemov, ki obdelujejo PII z velikim vplivom ali občutljive PII, in izid pregleda evidentirati v REG12.

4.2.4 [Both] System Owner / Application Owner mora najmanj letno pregledati uporabniški dostop do drugih sistemov, ki obdelujejo PII, in izid pregleda evidentirati v REG12.

4.2.5 [Both] System Owner / Application Owner mora odstraniti ali spremeniti dostop do PII v REG12 v enem delovnem dnevu po spremembi vloge, prenehanju razmerja, zaključku pogodbe ali ko dostop ni več potreben.

4.2.6 [Processor] Vendor / Procurement Owner mora v REG08 potrditi, da je dostop obdelovalca do PII naročnika omejen na dokumentirana navodila naročnika, preden se dostop omogoči ali spremeni.

4.2.7 [Subprocessor] Vendor / Procurement Owner mora v REG08 potrditi, da je dostop podobdelovalca do PII omejen na pooblaščene dejavnosti podobdelave, preden se dostop podobdelovalca omogoči ali spremeni.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Izjeme

9.1.1 [Both] Information Security Lead mora vsako izjemo od zahteve glede varnosti PII ali nadzora dostopa evidentirati v REG12, preden se izjema aktivira.

9.1.2 [Both] Data Protection Officer / Privacy Advisor mora pred odobritvijo svetovati glede varnostnih izjem za PII z višjim tveganjem v REG12.

9.1.3 [Both] Top Management mora pred aktivacijo odobriti varnostne izjeme za PII v REG12, kadar izjema vpliva na PII z velikim vplivom, občutljive PII, privilegirani dostop, šifriranje, beleženje ali nerešene visoko tvegane ranljivosti.

9.1.4 [Both] Information Security Lead mora v REG12 določiti datum poteka izjeme, nadomestno kontrolo in datum pregleda, preden se izjema odobri.

9.1.5 [Both] System Owner / Application Owner mora v REG12 odpraviti, obnoviti ali zapreti potekle varnostne izjeme za PII v petih delovnih dneh po poteku.

9.1.6 [Processor] Vendor / Procurement Owner mora varnostne izjeme obdelovalca ali podobdelovalca, ki vplivajo na PII naročnika, evidentirati v REG08 in REG12 pred sprejemom.

10. Uveljavljanje

10.1.1 [Both] Privacy Lead / PIMS Manager mora v REG12 evidentirati neskladnosti zaradi manjkajočih ali nepopolnih dokazil o varnosti PII v petih delovnih dneh po identifikaciji.

10.1.2 [Both] Information Security Lead mora v REG12 dodeliti lastništvo odprave odpovedi varnostnih kontrol za PII v petih delovnih dneh po validaciji.

10.1.3 [Both] System Owner / Application Owner mora v enem delovnem dnevu po validaciji onemogočiti ali omejiti nepooblaščen, čezmeren ali z dokazili nepodprt dostop do PII in ukrep evidentirati v REG12.

10.1.4 [Conditional] Incident Response Coordinator mora ukrepe izvrševanja povezati z REG10 v enem delovnem dnevu, kadar zadeva uveljavljanja vključuje domnevni ali potrjeni incident v zvezi s PII.

10.1.5 [Both] Top Management mora pred vodstvenim pregledom pregledati ponavljajoče se ali visoko tvegane neskladnosti glede varnosti PII v REG12.

11. Pregledovanje in vzdrževanje

11.1.1 [All] Privacy Lead / PIMS Manager mora skupaj z Information Security Lead najmanj letno pregledati to politiko in izid pregleda evidentirati v REG12.

11.1.2 [Both] Information Security Lead mora v REG12 pregledati osnovni nabor varnostnih zahtev za PII v 30 dneh po bistveni tehnološki spremembi, spremembi groženj, presoji, incidentu ali regulativni spremembi, ki vpliva na varnost PII.

11.1.3 [Both] System Owner / Application Owner mora v REG12 posodobiti dokazila o varnosti PII na ravni sistema v 30 dneh po bistveni spremembi arhitekture, dostopa, konfiguracije, ranljivosti ali beleženja.

11.1.4 [Processor] Vendor / Procurement Owner mora v REG08 pregledati dokazila o varnostnih odgovornostih obdelovalcev in podobdelovalcev za PII v 30 dneh po bistveni spremembi storitve, navodil naročnika ali podobdelovalca.

11.1.5 [All] Internal Audit / Compliance Reviewer mora preveriti dokazila o pregledu politike in izbrana dokazila o varnostnih kontrolah za PII v REG12 v skladu z odobrenim načrtom presoj.

12. Povezane politike

12.1 To politiko je treba brati skupaj z:

12.1.1 PII01 - Politika sistema upravljanja informacij o zasebnosti;

12.1.2 PII02 - Politika vlog, pristojnosti in odgovornosti za zasebnost;

12.1.3 PII03 - Politika popisa dejavnosti obdelave PII in pravne podlage;

12.1.4 PII07 - Politika ocene tveganj za zasebnost in DPIA;

12.1.5 PII08 - Politika varstva zasebnosti že pri načrtovanju in privzetega varstva zasebnosti;

12.1.6 PII09 - Politika zbiranja, uporabe, razkritja in deljenja PII;

12.1.7 PII10 - Politika hrambe, izbrisa in odstranjevanja PII;

12.1.8 PII12 - Politika upravljanja zasebnosti obdelovalcev, podobdelovalcev in tretjih oseb;

12.1.9 PII13 - Politika mednarodnih prenosov PII;

12.1.10 PII15 - Politika upravljanja incidentov in kršitev v zvezi s PII;

12.1.11 PII16 - Politika usposabljanja, ozaveščanja in usposobljenosti na področju zasebnosti;

12.1.12 PII17 - Politika dokumentiranih informacij in upravljanja dokazil PIMS;

12.1.13 PII18 - Politika spremljanja, presoje in izboljševanja PIMS.

13. Referenčni standardi in okviri

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].