					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII14					Naziv dokumenta: **Politika sigurnosti PII i kontrole pristupa**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard / propis	Točka / kontrola / članak	Primjenjivost	Vrsta obuhvata	Napomena
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planiranje i provedba sigurnosnih kontrola za PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Dokazi, praćenje i korektivne radnje
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitet i prava pristupa za obradu PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Zaštita krajnjih uređaja i sigurna autentifikacija
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Zapisivanje događaja i kriptografska zaštita
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Sigurnost aplikacija i sigurna arhitektura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Zaštita i pregled zapisa
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sigurnost, odgovornost i kontrole izvršitelja obrade
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 kontrola 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	Smjernice za provedbu sigurnosnih kontrola
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Načela informacijske sigurnosti i usklađenosti u području privatnosti

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	Sigurnosne kontrole za zaštitu PII

1. Opseg

1.1 Ova politika definira sigurnosne zahtjeve i zahtjeve kontrole pristupa specifične za PII za sustave, aplikacije, usluge, uređaje, okruženja u oblaku i operativne procese koji pohranjuju, prenose, obrađuju, pristupaju, administriraju ili štite PII.

1.2 Ova se politika primjenjuje na kontekste voditelja obrade, zajedničkog voditelja obrade, izvršitelja obrade i podizvršitelja obrade u kojima organizacija određuje, provodi, podržava ili se oslanja na sigurnosne kontrole za obradu PII.

1.3 Ova politika obuhvaća sljedeće domene sigurnosnih kontrola za PII:

1.3.1 polaznu osnovu sigurnosti PII i integraciju s postojećim politikama informacijske sigurnosti;

1.3.2 kontrolu pristupa;

1.3.3 autentifikaciju;

1.3.4 pristup s povišenim ovlastima;

1.3.5 šifriranje i sigurnu pohranu;

1.3.6 zapisivanje događaja i praćenje;

1.3.7 sigurnu konfiguraciju i upravljanje ranjivostima;

1.3.8 kontrole pristupa s krajnjih uređaja i iz oblaka;

1.3.9 povezivanje dokaza putem REG02, REG08, REG10 i REG12.

1.4 Ova politika ne zamjenjuje cjelovit sustav upravljanja informacijskom sigurnošću, politiku sigurnosti mreže, politiku sigurnog razvoja, politiku sigurnosnog kopiranja, politiku krajnjih uređaja, politiku sigurnosti oblaka, kriptografski standard, postupak upravljanja ranjivostima ili postupak odgovora na incidente. Ako takve politike već postoje, ova politika definira povezivanje specifično za PII i zahtjeve za dokazima potrebne za osiguranje PIMS.

1.5 Ova politika ne duplicira:

1.5.1 popis aktivnosti obrade PII i vlasništvo nad pravnom osnovom iz PII03;

1.5.2 metodologiju procjene rizika za privatnost i DPIA iz PII07;

1.5.3 kontrolne točke ugrađene zaštite privatnosti iz PII08;

1.5.4 pravila prikupljanja, uporabe, otkrivanja i dijeljenja iz PII09;

1.5.5 provedbu zadržavanja, brisanja i zbrinjavanja iz PII10;

1.5.6 upravljanje životnim ciklusom izvršitelja obrade iz PII12;

1.5.7 kontrole mehanizama međunarodnog prijenosa iz PII13;

1.5.8 tijek rada za incidente i povrede iz PII15;

1.5.9 upravljanje dokumentiranim informacijama iz PII17;

1.5.10 upravljanje praćenjem, revizijom i poboljšanjem PIMS iz PII18.

1.6 Za potrebe ove politike, operativni dnevnički zapisi, izlazni rezultati sigurnosnih alata, izvozi pregleda pristupa, izvješća o ranjivostima i konfiguracijski dokazi izvori su dokaza koji se prilažu, sažimaju ili referenciraju u kanonskim dokaznim objektima. Oni nisu zasebni PIMS registri.

2. Svrha

2.1 Svrha ove politike jest osigurati da je PII zaštićen odgovarajućim, riziku prilagođenim i revizijski provjerljivim sigurnosnim kontrolama i kontrolama pristupa tijekom cijele obrade.

2.2 Ova politika omogućuje organizaciji da dokaže da se sigurnosne kontrole za PII planiraju, provode, pregledavaju, prate i poboljšavaju putem REG02, REG08, REG10 i REG12 bez stvaranja dupliciranih sigurnosnih registara ili zamjene postojećih politika informacijske sigurnosti.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 definirati polaznu osnovu kontrole pristupa PII za sustave i aktivnosti obrade;

3.1.2 osigurati da su kontrole autentifikacije primjerene osjetljivosti PII i kontekstu pristupa;

3.1.3 definirati zahtjeve pregleda za pristup PII s povišenim ovlastima i redovni pristup PII;

3.1.4 definirati očekivanja za šifriranje i sigurnu pohranu PII u mirovanju, u prijenosu te u relevantnim kontekstima oblaka ili krajnjih uređaja;

3.1.5 definirati očekivanja za zapisivanje događaja i praćenje pristupa PII, izmjena PII i administriranja PII;

3.1.6 definirati zahtjeve za dokazima o sigurnoj konfiguraciji i ranjivostima za sustave koji obrađuju PII;

3.1.7 definirati očekivanja u pogledu pristupa s krajnjih uređaja i iz oblaka bez stvaranja cjelovite politike krajnjih uređaja ili sigurnosti oblaka;

3.1.8 povezati sumnje na sigurnosne incidente povezane s PII s REG10 bez dupliciranja tijeka rada za incidente;

3.1.9 integrirati se s postojećim politikama informacijske sigurnosti kada su dostupne;

3.1.10 održavati dokaze spremne za reviziju koristeći samo REG02, REG08, REG10 i REG12.

4. Izjave politike

4.1 Polazna osnova sigurnosti PII i integracija s ISMS

4.1.1 [Both] Information Security Lead MUST definirati polaznu osnovu sigurnosti PII za svaki sustav ili uslugu koji obrađuju PII u REG12 prije nego što sustav ili usluga uđu u produkcijski rad ili se značajno promijene.

4.1.2 [Both] System Owner / Application Owner MUST zabilježiti lokaciju dokaza o provedenoj sigurnosnoj kontroli za PII u REG12 prije oslanjanja na postojeću kontrolu informacijske sigurnosti za potrebe osiguranja PIMS.

4.1.3 [Controller] Process Owner / Business Owner MUST identificirati osjetljivost PII, kontekst obrade i potrebu za pristupom u REG02 prije zahtijevanja novog ili značajno izmijenjenog pristupa PII.

4.1.4 [Processor] Vendor / Procurement Owner MUST zabilježiti sigurnosne upute klijenta, granice odgovornosti klijenta i sigurnosne obveze izvršitelja obrade u REG08 prije početka ili značajne promjene pristupa izvršitelja obrade PII klijenta.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST provjeriti da su sigurnosni dokazi za PII povezani s REG02, REG08, REG10 ili REG12 prije prihvaćanja aktivnosti obrade kao revizijski provjerljive u okviru PIMS.

4.2 Polazna osnova kontrole pristupa

4.2.1 [Both] System Owner / Application Owner MUST ograničiti pristup PII na odobrene uloge i ovlaštene korisnike zabilježene ili sljedive u REG02 ili REG12 prije omogućavanja pristupa.

4.2.2 [Both] Process Owner / Business Owner MUST odobriti poslovnu svrhu pristupa PII u REG02 ili REG12 prije nego što System Owner / Application Owner dodijeli pristup.

4.2.3 [Both] System Owner / Application Owner MUST pregledati korisnički pristup sustavima koji obrađuju PII visokog utjecaja ili osjetljivi PII najmanje tromjesečno i zabilježiti ishod pregleda u REG12.

4.2.4 [Both] System Owner / Application Owner MUST pregledati korisnički pristup drugim sustavima koji obrađuju PII najmanje jednom godišnje i zabilježiti ishod pregleda u REG12.

4.2.5 [Both] System Owner / Application Owner MUST ukloniti ili izmijeniti pristup PII u REG12 u roku od jednog radnog dana nakon promjene uloge, prestanka radnog odnosa, završetka ugovora ili kada pristup više nije potreban.

4.2.6 [Processor] Vendor / Procurement Owner MUST potvrditi u REG08 da je pristup izvršitelja obrade PII klijenta ograničen na dokumentirane upute klijenta prije omogućavanja ili izmjene pristupa.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST potvrditi u REG08 da je pristup podizvršitelja obrade PII ograničen na ovlaštene aktivnosti podizvršenja obrade prije omogućavanja ili izmjene pristupa podizvršitelja obrade.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Iznimke

9.1.1 [Both] Information Security Lead MUST zabilježiti svaku iznimku od zahtjeva sigurnosti PII ili kontrole pristupa u REG12 prije aktivacije iznimke.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST savjetovati o sigurnosnim iznimkama višeg rizika povezanim s PII u REG12 prije odobrenja.

9.1.3 [Both] Top Management MUST odobriti sigurnosne iznimke povezane s PII u REG12 prije aktivacije kada iznimka utječe na PII visokog utjecaja, osjetljivi PII, pristup s povišenim ovlastima, šifriranje, zapisivanje događaja ili neriješene visokorizične ranjivosti.

9.1.4 [Both] Information Security Lead MUST definirati istek iznimke, kompenzacijsku kontrolu i datum pregleda u REG12 prije odobrenja iznimke.

9.1.5 [Both] System Owner / Application Owner MUST otkloniti, obnoviti ili zatvoriti istekle sigurnosne iznimke povezane s PII u REG12 u roku od pet radnih dana nakon isteka.

9.1.6 [Processor] Vendor / Procurement Owner MUST zabilježiti sigurnosne iznimke izvršitelja obrade ili podizvršitelja obrade koje utječu na PII klijenta u REG08 i REG12 prije prihvaćanja.

10. Provedba i usklađenost

10.1.1 [Both] Privacy Lead / PIMS Manager MUST zabilježiti nesukladnosti za nedostajuće ili nepotpune sigurnosne dokaze povezane s PII u REG12 u roku od pet radnih dana od identifikacije.

10.1.2 [Both] Information Security Lead MUST dodijeliti vlasništvo nad otklanjanjem neuspjeha sigurnosnih kontrola za PII u REG12 u roku od pet radnih dana od potvrde.

10.1.3 [Both] System Owner / Application Owner MUST onemogućiti ili ograničiti neovlašten, pretjeran ili nepotkrijepljen pristup PII u roku od jednog radnog dana od potvrde i zabilježiti radnju u REG12.

10.1.4 [Conditional] Incident Response Coordinator MUST povezati provedbene radnje s REG10 u roku od jednog radnog dana kada se predmet provedbe odnosi na sumnjivi ili potvrđeni incident povezan s PII.

10.1.5 [Both] Top Management MUST pregledati ponavljajuće ili visokorizične sigurnosne nesukladnosti povezane s PII u REG12 prije preispitivanja od strane uprave.

11. Pregled i održavanje

11.1.1 [All] Privacy Lead / PIMS Manager MUST pregledati ovu politiku s Information Security Lead najmanje jednom godišnje i zabilježiti ishod pregleda u REG12.

11.1.2 [Both] Information Security Lead MUST pregledati polaznu osnovu sigurnosti PII u REG12 u roku od 30 dana nakon značajne tehnološke promjene, promjene prijetnji, revizije, incidenta ili regulatorne promjene koja utječe na sigurnost PII.

11.1.3 [Both] System Owner / Application Owner MUST ažurirati sigurnosne dokaze za PII na razini sustava u REG12 u roku od 30 dana nakon značajne promjene arhitekture, pristupa, konfiguracije, ranjivosti ili zapisivanja događaja.

11.1.4 [Processor] Vendor / Procurement Owner MUST pregledati dokaze o sigurnosnim odgovornostima izvršitelja obrade i podizvršitelja obrade za PII u REG08 u roku od 30 dana nakon značajne promjene usluge, upute klijenta ili podizvršitelja obrade.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST provjeriti dokaze o pregledu politike i odabrane dokaze o sigurnosnim kontrolama za PII u REG12 u skladu s odobrenim planom revizije.

12. Povezane politike

12.1 Ovu politiku treba čitati zajedno sa sljedećim politikama:

12.2 PII01 - Politika sustava upravljanja informacijama o privatnosti;

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost;

12.4 PII03 - Politika popisa aktivnosti obrade PII i pravne osnove;

12.5 PII07 - Politika procjene rizika za privatnost i DPIA;

12.6 PII08 - Politika ugrađene i zadane zaštite privatnosti;

12.7 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja PII;

12.8 PII10 - Politika zadržavanja, brisanja i zbrinjavanja PII;

12.9 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana;

12.10 PII13 - Politika međunarodnog prijenosa PII;

12.11 PII15 - Politika upravljanja incidentima i povredama povezanima s PII;

12.12 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencija u području privatnosti;

12.13 PII17 - Politika upravljanja dokumentiranim informacijama i dokazima PIMS;

12.14 PII18 - Politika praćenja, revizije i poboljšanja PIMS.

13. Referentni standardi i 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].