					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P01					Naziv dokumenta: **Politika informacijske sigurnosti**							
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**

1. Svrha

1.1 Ova politika utvrđuje sveobuhvatnu opredijeljenost organizacije informacijskoj sigurnosti uspostavom formalnog sustava upravljanja informacijskom sigurnošću (ISMS).

1.2 Njome se određuju strateški smjer i temeljni zahtjevi za zaštitu povjerljivosti, cjelovitosti, dostupnosti i otpornosti cjelokupne informacijske imovine u fizičkim, digitalnim i oblačnim okruženjima.

1.3 Ova politika ispunjava zahtjeve točaka 5.1 i 5.2 norme ISO/IEC 27001:2022 time što izražava namjeru vodstva, opredijeljenost najvišeg rukovodstva i usklađenost sigurnosnih aktivnosti s ciljevima organizacije.

1.4 Ova politika služi kao mjerodavna referenca za sve podređene politike, standarde i postupke unutar ISMS-a te je ključna za uspostavu sigurnosnog okruženja koje se temelji na riziku, usklađenosti i kontinuiranom poboljšavanju.

2. Opseg

2.1 Ova politika primjenjuje se na sve osobe, imovinu i procese definirane unutar opsega ISMS-a, uključujući:

2.1.1 sve poslovne jedinice, odjele, podružnice i poslovnice

2.1.2 sve zaposlenike, ugovorne izvođače, privremeno osoblje, konzultante i pružatelje usluga trećih strana

2.1.3 sve podatke, informacijske sustave, aplikacije, infrastrukturu i komunikacijske kanale

2.1.4 sva fizička, oblačna, udaljena i hibridna okruženja u kojima se podaci društva obrađuju ili kojima se pristupa

2.2 Ova je politika obvezujuća za sve subjekte koji postupaju s informacijama organizacije te se primjenjuje na sve faze životnog ciklusa informacija, od nastanka i prijenosa do pohrane i zbrinjavanja.

2.3 Sva isključenja ili ograničenja iz ovog opsega moraju biti dokumentirana u Izjavi o opsegu ISMS-a i obrazložena uz formalno odobrenje izvršnog rukovodstva.

3. Ciljevi

3.1 Uspostaviti ISMS usklađen s normom ISO/IEC 27001:2022 i sposoban podržati odlučivanje temeljeno na riziku u cijeloj organizaciji.

3.2 Osigurati da načela povjerljivosti, cjelovitosti i dostupnosti budu ugrađena u sve aktivnosti organizacije, sustave i partnerstva.

3.3 Omogućiti usklađenost s regulatornim i ugovornim zahtjevima utvrđivanjem mjerljivih sigurnosnih ciljeva utemeljenih na politici i njihovom integracijom u poslovne operacije.

3.4 Smanjiti vjerojatnost i učinak incidenata informacijske sigurnosti primjenom djelotvornih preventivnih, detektivnih i korektivnih kontrola.

3.5 Poticati kontinuirano povećanje zrelosti informacijske sigurnosti putem definiranih pokazatelja uspješnosti, ishoda revizije i preispitivanja uprave.

3.6 Promicati kulturu odgovornosti, svijesti i otpornosti u kojoj su sigurnosne odgovornosti jasno razumljive i izvršavaju ih svi djelatnici.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava i potvrđuje Politiku informacijske sigurnosti i okvir ISMS-a.

4.1.2 Osigurava usklađenost između sigurnosnih ciljeva i poslovne strategije.

4.1.3 Daje primjer i promiče snažnu kulturu informacijske sigurnosti.

4.1.4 Preispituje i odobrava značajne promjene opsega ISMS-a, obrade rizika i strukture upravljanja.

4.2 Glavni direktor informacijske sigurnosti (CISO) / voditelj ISMS-a

4.2.1 Odgovoran je za ISMS i održava ovu politiku u skladu s normom ISO/IEC 27001.

4.2.2 Vodi procjenu rizika, provedbu kontrola i procese kontinuiranog poboljšavanja.

4.2.3 Osigurava međufunkcionalnu koordinaciju sigurnosnih aktivnosti i nadzire podređene politike.

4.2.4 Izvješćuje najviše rukovodstvo o statusu ISMS-a, incidentima, rezultatima revizije i pokazateljima.

4.2.5 Osigurava da se pregledi i ažuriranja politike provode u skladu s odjeljkom 9 ovog dokumenta.

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

9. Pregled i ažuriranje zahtjeva

9.1 Učestalost pregleda

9.1.1 Ova politika mora se pregledavati najmanje jednom godišnje ili nakon bilo kojeg od sljedećih pokretača:

9.1.1.1 značajnih promjena zakonskih, regulatornih ili ugovornih obveza

9.1.1.2 značajnih promjena u profilu rizika organizacije

9.1.1.3 ishoda unutarnjih ili vanjskih revizija

9.1.1.4 velikih incidenata ili neuspjeha kontrola

9.2 Ovlasti i postupak pregleda

9.2.1 Glavni direktor informacijske sigurnosti (CISO) ili imenovani voditelj ISMS-a vodi postupak pregleda.

9.2.2 Ulazni podaci za pregled moraju uključivati:

9.2.2.1 rezultate unutarnje revizije

9.2.2.2 trendove procjene rizika

9.2.2.3 promjene poslovnih procesa i tehnologije

9.2.2.4 uspješnost u odnosu na KPI-je i pragove rizika

9.2.3 Sva ažuriranja moraju:

9.2.3.1 biti pod verzijskom kontrolom i dokumentirana

9.2.3.2 biti odobrena od strane izvršnog rukovodstva

9.2.3.3 biti distribuirana svim pogođenim stranama putem službenih komunikacijskih kanala

9.2.3.4 pokrenuti potrebna ažuriranja podređene dokumentacije i obuke

10. Povezane politike i poveznice

10.1 Ova temeljna politika izravno je povezana sa sljedećim organizacijskim sigurnosnim politikama i okvirima:

10.1.1 P2 – Politika uloga i odgovornosti upravljanja: definira strukturu upravljanja i hijerarhiju ovlasti na koje se upućuje u ovom dokumentu.

10.1.2 P3 – Politika prihvatljive uporabe: uređuje usklađenost ponašanja i prihvatljivo postupanje s informacijskom imovinom.

10.1.3 P4 – Politika kontrole pristupa: operativno uređuje kontrole povezane s pristupom koje proizlaze iz ove krovne politike.

10.1.4 P6 – Politika upravljanja rizicima: pruža kontekst temeljen na riziku za odabir kontrola i prihvaćanje preostalog rizika.

10.1.5 P33 – Politika praćenja revizije i usklađenosti: detaljno uređuje kako mehanizmi internog osiguranja potvrđuju provedbu politike.

10.2 Ove međuovisnosti osiguravaju sveobuhvatnu usklađenost i sljedivost u okviru ISMS-a te podupiru jedinstveno upravljanje rizikom i usklađenošću.

11. Referentni standardi i okviri

11.1 Ova Politika informacijske sigurnosti formalno je usklađena sa sljedećim standardima i okvirima kako bi se osigurala potpuna usklađenost, spremnost za reviziju i mogućnost obrazlaganja pred regulatornim tijelima:

11.2 ISO/IEC 27001

11.2.1 Točka 5.1 – Vodstvo i opredijeljenost: ova politika pokazuje opredijeljenost najvišeg rukovodstva informacijskoj sigurnosti te definira odgovornosti i raspodjelu resursa za ISMS.

11.2.2 Točka 5.2 – Politika informacijske sigurnosti: ovaj dokument služi kao formalna sigurnosna politika organizacije, usklađena s utvrđenim sigurnosnim ciljevima, poslovnom strategijom i zahtjevima norme ISO/IEC 27001.

11.2.3 Točka 6.1 – Radnje za rješavanje rizika i prilika: pristup temeljen na riziku, kako je odražen u ovoj politici, osigurava da se sigurnosni resursi primjenjuju razmjerno prijetnjama.

11.2.4 Točka 9.2 – Unutarnja revizija i točka 10 – Poboljšavanje: ova politika ugrađena je u životni ciklus kontinuiranog poboljšavanja organizacije i podložna je potvrdi kroz unutarnju reviziju.

11.2.5 ISO/IEC 27002:2022 – Kontrola 5.1: utvrđuje smjernice za uspostavu i održavanje sigurnosnih politika. Ova politika odražava preporuke norme ISO 27002 za hijerarhijsku dokumentaciju, cikluse pregleda i provedivost.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politika i postupci sigurnosnog planiranja): ova politika ispunjava zahtjev za izradom, distribucijom i pregledom formalne politike informacijske sigurnosti na razini cijele organizacije.

11.3.2 PM-1 do PM-5: obuhvaća upravljanje na razini programa, uključujući uloge u informacijskoj sigurnosti, raspodjelu resursa, strategiju rizika i integraciju sigurnosnog planiranja u operacije organizacije.

11.4 GDPR EU (2016/679)

11.4.1 Članak 5(2): provodi načelo odgovornosti. Ova politika definira odgovorne strane i sljedive provedbene radnje.

11.4.2 Članak 24: zahtijeva provedbu tehničkih i organizacijskih mjera, uključujući politike usklađene s rizikom.

11.4.3 Članak 32: podupire provedbu odgovarajućih mjera za osiguranje sigurnosti osobnih podataka tijekom cijelog njihova životnog ciklusa.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(a): obvezuje subjekte na provedbu dokumentirane sigurnosne politike koja obuhvaća upravljanje rizicima i upravljanje. Ova politika ispunjava taj zahtjev i podupire širu spremnost za kibernetičku sigurnost i zaštitu kritične infrastrukture.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 5(2): zahtijeva dokumentirani okvir unutarnjih kontrola za upravljanje ICT rizicima. Ova politika podupire usklađenost financijskog sektora dodjelom uloga, kontrola i nadzornih funkcija usklađenih s očekivanjima upravljanja iz Uredbe DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Uspostava okvira upravljanja: ova politika podupire upravljanje organizacijom definiranjem uloga u ISMS-u, opredijeljenosti vodstva i strateških ciljeva.

11.7.2 APO01 – Okvir upravljanja: podupire uspostavu i rad strukturiranog ISMS-a.

11.7.3 APO12 – Upravljanje rizicima: pruža osnovu za upravljanje rizicima informacijske sigurnosti.

11.7.4 MEA01/MEA03 – Praćenje, vrednovanje i procjena: jača kontinuirano vrednovanje uspješnosti i praćenje unutarnjih kontrola kroz provedbu usklađenosti s politikom.