					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P02					Naziv dokumenta: **Politika uloga i odgovornosti u upravljanju**							
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/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 5.3; Dodatak A, kontrola 5	
ISO/IEC 27002:2022	Kontrola 5	
NIST SP 800-53 Rev.5	PL-1 do PL-4, PM-1 do PM-13	
GDPR EU	Članci 5(1)(f), 24, 37	
Direktiva EU NIS2	Članak 21(2)(a)	
Uredba EU DORA	Članak 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Svrha

1.1 Ova politika definira model upravljanja, organizacijske uloge i odgovornosti potrebne za uspostavu i djelotvorno funkcioniranje sustava upravljanja informacijskom sigurnošću (ISMS).

1.2 Ovom politikom uspostavljaju se jasne linije odgovornosti, ovlasti za donošenje odluka i kanali eskalacije kako bi informacijska sigurnost bila ugrađena na svim razinama organizacije i usklađena sa strateškim poslovnim ciljevima.

1.3 Ova politika provodi zahtjeve norme ISO/IEC 27001:2022, točke 5.3 i kontrole A.5.2, osiguravajući da su odgovornosti za aktivnosti povezane sa sigurnošću jasno dodijeljene, dokumentirane, komunicirane i predmet periodičnog pregleda.

1.4 Ova politika također pruža temelj za integrirano upravljanje s drugim područjima, kao što su upravljanje rizicima, usklađenost, IT operacije i pravni poslovi.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve pojedince i subjekte uključene u upravljanje, provedbu i nadzor informacijske sigurnosti unutar opsega ISMS-a. To uključuje:

2.1.1 najviše rukovodstvo, više rukovodstvo i članove odbora

2.1.2 voditelja ISMS-a, CISO-a i vlasnike kontrola

2.1.3 vlasnike procesa i imovine

2.1.4 ugovorne izvođače i pružatelje usluga trećih strana s delegiranim sigurnosnim odgovornostima

2.2 Obuhvaća i interne i eksterno pružene funkcije (npr. vanjski centar za sigurnosne operacije, administratore platformi u oblaku) kada su uloge upravljanja formalno dodijeljene ili ugovorno definirane.

2.3 Ova politika primjenjuje se i na organizacijske jedinice, odjele i projektne timove koji upravljaju imovinom, sustavima ili uslugama relevantnima za sigurnost ili na njih utječu.

3. Ciljevi

3.1 Osigurati da su uloge i odgovornosti u području informacijske sigurnosti formalno definirane, dodijeljene, komunicirane i dokumentirane.

3.2 Održavati model upravljanja koji provodi razdvajanje dužnosti (SoD), uklanja sukobe interesa i omogućuje eskalaciju neriješenih sigurnosnih pitanja.

3.3 Osigurati da su odgovornost i ovlasti za sigurnosne odluke raspodijeljene u skladu s utjecajem na poslovanje i organizacijskom strukturom.

3.4 Uspostaviti okvir za upravljanje delegiranjem, promjenama uloga i pregledom dodijeljenih odgovornosti.

3.5 Pružiti dionicima, uključujući regulatore, revizore i klijente, razumno uvjerenje da se informacijskom sigurnošću upravlja djelotvorno i u skladu s primjenjivim standardima.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo (najviše rukovodstvo)

4.1.1 Osigurava strateški nadzor, dodjeljuje resurse i osigurava usklađenost između ciljeva ISMS-a i poslovnih ciljeva.

4.1.2 Odobrava ključnu dokumentaciju ISMS-a, uključujući Politiku informacijske sigurnosti, planove obrade rizika i odluke o korektivnim radnjama nakon revizije.

4.1.3 Sudjeluje u preispitivanjima sustava upravljanja informacijskom sigurnošću od strane uprave i eskalira odluke koje zahtijevaju odobrenje na razini odbora.

4.1.4 Promiče kulturu sigurnosti i potiče pridržavanje načela upravljanja sigurnošću u cijeloj organizaciji.

4.2 Odbor za upravljanje informacijskom sigurnošću

4.2.1 Djeluje kao međufunkcionalno tijelo upravljanja za nadzor ISMS-a.

4.2.2 Pregledava profil rizika, djelotvornost kontrola, nalaze revizije i strateške sigurnosne inicijative.

4.2.3 Olakšava koordinaciju među odjelima (npr. IT, pravni poslovi, ljudski resursi, rizici, usklađenost, operacije).

4.2.4 Odobrava pragove eskalacije, raspodjelu proračuna i izmjene politika koje zahtijevaju doprinos izvršnog rukovodstva.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Raspored pregleda

9.1.1 Ova politika mora se pregledati najmanje jednom godišnje ili nakon nastupa sljedećih događaja:

9.1.1.1 promjene organizacijske strukture ili izvršnog tima

9.1.1.2 proširenje ili redefiniranje opsega ISMS-a

9.1.1.3 regulatorne promjene koje utječu na dodjelu uloga ili nadzor

9.1.1.4 značajni nalazi revizije ili incidenti povezani s propustima u upravljanju

9.2 Postupak pregleda i odobravanja

9.2.1 Voditelj ISMS-a pokreće i vodi postupak pregleda, uključujući prikupljanje doprinosa dionika i povratnih informacija iz revizije.

9.2.2 Predložena ažuriranja mora pregledati Odbor za upravljanje informacijskom sigurnošću, a formalno odobriti izvršno rukovodstvo.

9.2.3 Svaka verzija mora se pratiti u Registru dokumenata ISMS-a i uključivati sljedeće metapodatke:

9.2.3.1 identifikator politike i naslov

9.2.3.2 broj verzije i sažetak promjena

9.2.3.3 datum stupanja na snagu i datum sljedećeg pregleda

9.2.3.4 vlasnika politike i odobravatelja

9.2.3.5 razinu klasifikacije dokumenta

9.2.3.6 povijest zadržavanja i arhiviranja

10. Povezane politike i poveznice

10.1 Ovu politiku treba tumačiti zajedno sa sljedećim politikama:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja cjelokupni program sigurnosti i utvrđuje odgovornosti rukovodstva za potvrđivanje politike i strateški nadzor.

10.1.2 P5 – Politika upravljanja promjenama: osigurava da promjene struktura upravljanja, uloga ili odgovornosti podliježu dokumentiranom odobrenju i pregledu rizika.

10.1.3 P6 – Politika upravljanja rizicima: identificira i obrađuje rizike upravljanja koji proizlaze iz sukoba uloga, nedodijeljenih dužnosti ili izostanka eskalacije.

10.1.4 P7 – Politika uvođenja u posao i prestanka radnog odnosa: provodi procese dodjele i ukidanja kontrola tijekom promjena u životnom ciklusu osoblja.

10.1.5 P33 – Politika praćenja revizije i usklađenosti: podupire neovisni pregled djelotvornosti upravljanja i provedbu korektivnih radnji za neusklađenost.

10.2 Ove politike zajedno podupiru jedinstven i provediv okvir upravljanja ISMS-om.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s globalno priznatim standardima i okvirima za upravljanje informacijskom sigurnošću i odgovornost za uloge. Osigurava sljedivost prema regulatornim zahtjevima i zahtjevima za certifikaciju te podupire dokazivu strukturu ISMS-a.

11.2 ISO/IEC 27001

11.2.1 Točka 5.3 – Organizacijske uloge, odgovornosti i ovlasti: ova politika ispunjava zahtjev da se uloge relevantne za informacijsku sigurnost jasno dodijele, komuniciraju i dokumentiraju.

11.2.2 Točka 9.3 – Preispitivanje od strane uprave: ova politika provodi izvršni nadzor nad ulogama ISMS-a i upravljanjem kroz tromjesečne i godišnje preglede.

11.2.3 Dodatak A, kontrola 5.2 – Uloge i odgovornosti u informacijskoj sigurnosti: definira uloge na tehničkoj, operativnoj i strateškoj razini radi osiguravanja razdvajanja dužnosti, vlasništva nad rizikom i sljedive odgovornosti.

11.3 ISO/IEC 27002:2022 – Kontrola 5

11.3.1 Daje smjernice za provedbu dodjele odgovornosti za informacijsku sigurnost unutar organizacije. Ova politika preuzima te smjernice definiranjem vrsta uloga, pravila delegiranja, postupaka eskalacije i mehanizama pregleda.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 do PL-4: provode potrebu za formalnom planskom dokumentacijom, uključujući politike koje definiraju upravljanje i dodjeljuju sigurnosne odgovornosti.

11.4.2 PM-1 (plan programa informacijske sigurnosti) i PM-2 (viši službenik za informacijsku sigurnost): odraženi su u ovoj politici kroz dodjelu uloge CISO-a / voditelja ISMS-a i formalnih upravljačkih uloga.

11.4.3 PM-5 do PM-13: ova politika ispunjava zahtjeve za dokumentiranje uloga, uloge upravljanja rizicima na razini poduzeća, nadzor nad upravljanjem konfiguracijom i integraciju s poslovnim funkcijama.

11.5 GDPR EU (2016/679)

11.5.1 Članak 5(1)(f): zahtijeva da osobni podaci budu zaštićeni od neovlaštene ili nezakonite obrade. Ova politika osigurava da su osobe odgovorne za zaštitu podataka jasno određene i pod nadzorom.

11.5.2 Članak 24: zahtijeva odgovarajuće organizacijske mjere, uključujući strukture upravljanja.

11.5.3 Članak 37: zahtijeva imenovanje službenika za zaštitu podataka (DPO), što mora biti odraženo u okviru upravljanja organizacije i registru odgovornosti.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članak 21(2)(a): nalaže da subjekti uspostave politike o analizi rizika i sigurnosti informacijskih sustava, uključujući odgovornosti specifične za uloge. Ova politika definira takve uloge i njihove mehanizme upravljanja.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članak 5 – okvir upravljanja i unutarnjih kontrola: zahtijeva formalnu dodjelu odgovornosti za upravljanje IKT rizicima, uloge u donošenju odluka i kanale izvješćivanja. Ova politika pruža temelj za upravljanje ulogama povezanima sa sigurnošću u IKT okruženjima.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: ova politika osigurava da ISMS ima jasno definiranu strukturu upravljanja usklađenu s potrebama organizacije.

11.8.2 EDM02 – Ensured Benefits Delivery: usklađuje sigurnosne aktivnosti temeljene na ulogama sa strateškim i operativnim ciljevima te osigurava odgovornost i mjerljive ishode.

11.8.3 APO01 – Managed I&T Management Framework i APO12 – Managed Risk: ova politika podupire strukturirano upravljanje ulogama informacijske sigurnosti unutar šireg okvira upravljanja IT-jem i rizicima.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: ugrađuje mehanizme pregleda za provjeru da su upravljačke uloge djelotvorne, ažurne i da se provode.