					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P02S					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	
ISO/IEC 27002:2022	Kontrole: 5.2, 5.3, 5.4	
GDPR EU	Članci 5(2), 32	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EU GDPR	Članci 5(2), 32	

1. Svrha

1.1 Ova politika definira način na koji se odgovornosti za upravljanje informacijskom sigurnošću dodjeljuju, delegiraju i nadziru unutar organizacije kako bi se osigurala potpuna usklađenost s normom ISO/IEC 27001:2022 i drugim regulatornim obvezama.

1.2 Osigurava odgovornost na svim razinama i podupire operativnu učinkovitost jasnim utvrđivanjem odgovorne osobe za svaku funkciju povezanu sa sigurnošću.

1.3 Ova politika povećava spremnost za reviziju i jača povjerenje korisnika dokazivanjem formaliziranog upravljanja sigurnošću, uključujući organizacije s ograničenim tehničkim resursima ili ugovorenim vanjskim IT uslugama.

2. Opseg

2.1 Ova politika primjenjuje se na sve osobe koje rukuju sustavima ili podacima organizacije, uključujući:

2.1.1 vlasnike poslovanja i glavne direktore

2.1.2 zaposlenike i ugovorne izvođače

2.1.3 vanjske pružatelje IT usluga ili konzultante

2.2 Obuhvaća sve sustave, okruženja i usluge koji se upotrebljavaju za obradu, prijenos ili pohranu poslovnih informacija ili informacija o korisnicima, uključujući:

2.2.1 uredsku IT infrastrukturu i uređaje za rad na daljinu

2.2.2 platforme u oblaku i usluge elektroničke pošte

2.2.3 fizičku dokumentaciju i zajedničke mrežne diskove

2.3 Opseg uključuje interne aktivnosti i aktivnosti povjerene vanjskim izvršiteljima koje se odnose na upravljanje informacijskom sigurnošću.

3. Ciljevi

3.1 Uspostaviti jasnu odgovornost za sve zadaće povezane sa sigurnošću, uključujući upravljanje politikama, kontrolu pristupa, upravljanje incidentima i nadzor.

3.2 Omogućiti učinkovito razdvajanje dužnosti (SoD) radi smanjenja sukoba interesa ili rizika od prijevare.

3.3 Osigurati da su sigurnosne zadaće i uloge jasno dokumentirane te da se redovito preispituju.

3.4 Omogućiti informirano odlučivanje, eskalaciju i nadzor nad IT i sigurnosnim rizicima.

3.5 Poduprijeti certifikaciju prema normi ISO/IEC 27001:2022 i izgraditi povjerenje korisnika, partnera i revizora.

4. Uloge i odgovornosti

4.1 Glavni direktor / vlasnik poslovanja

4.1.1 Snosi punu odgovornost za provedbu i nadzor ove politike.

4.1.2 Odobrava sve sigurnosne uloge, odgovornosti i odluke o delegiranju.

4.1.3 Nadzire usklađenost i donosi konačne odluke o iznimkama od politike i eskalacijama.

4.2 Imenovani koordinator informacijske sigurnosti (ako je imenovan)

4.2.1 Može biti zaposlenik ili pouzdani konzultant.

4.2.2 Tu ulogu može preuzeti glavni direktor ili vanjski pružatelj usluga u mikroposlovnim okruženjima.

4.2.3 Podržava svakodnevnu provedbu kontrole pristupa, upravljanje incidentima ili osnovne tehničke sigurnosne zadaće.

4.2.4 O svim sigurnosnim pitanjima ili rizicima izravno izvješćuje glavnog direktora.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled

9.1.1 Glavni direktor mora pregledati ovu politiku svakih 12 mjeseci kako bi osigurao da ona i dalje odražava pravne obveze, operativne potrebe i zahtjeve certifikacije prema normi ISO/IEC 27001.

9.2 Izvanredni pregledi

9.2.1 Pregledi se moraju provesti i kada:

9.2.1.1 nastupe velike organizacijske promjene

9.2.1.2 se uvede novi pružatelj usluga

9.2.1.3 nastane ozbiljan sigurnosni incident

9.2.1.4 se ažuriraju propisi kao što su Opća uredba o zaštiti podataka, Direktiva EU NIS2 ili Uredba EU DORA

9.3 Upravljanje verzijama i dokumentacija

9.3.1 Svi pregledi moraju uključivati:

9.3.1.1 datum pregleda

9.3.1.2 sažetak svih promjena

9.3.1.3 potpis glavnog direktora ili dokumentirano odobrenje glavnog direktora

9.3.1.4 arhivirane prethodne verzije za potrebe revizijskog traga

9.4 Obavještavanje o promjenama

9.4.1 Sva ažuriranja politike moraju se bez odgode priopćiti osoblju i pružateljima usluga putem poruka elektroničke pošte, internih portala ili službenih obavijesti.

10. Povezane politike i poveznice

10.1 Ovu politiku treba provoditi zajedno sa sljedećim SME politikama radi pune učinkovitosti:

10.1.1 P4S – Politika kontrole pristupa: definira kako se pristup odobrava, kojim se pristupom upravlja i kako se ukida te je izravno povezana s dodijeljenim ulogama i nadzorom.

10.1.2 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: jača odgovornosti i očekivanja specifična za ulogu.

10.1.3 P17S – Politika zaštite podataka i privatnosti: utvrđuje pravne obveze prema GDPR-u koje se dodjeljuju ulogama definiranima ovom politikom upravljanja.

10.1.4 P30S – Politika upravljanja incidentima: zahtijeva jasno definirane odgovornosti za prijavljivanje, eskalaciju i rješavanje incidenata.

10.2 Zajedno, ove politike omogućuju dosljednu provedbu, internu odgovornost i vanjsku usklađenost.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 5.3 – Organizacijske uloge, odgovornosti i ovlasti: zahtijeva da uloge budu jasno dodijeljene i podržane od strane najvišeg rukovodstva.

11.2 ISO/IEC 27002

11.2.1 Kontrole 5.2–5.4: zahtijevaju jasno dokumentiranje uloga u području informacijske sigurnosti, razdvajanje dužnosti i rukovoditeljski nadzor.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: uspostavlja sveobuhvatan program informacijske sigurnosti s definiranim odgovornostima.

11.3.2 PL-1 do PL-4: zahtijevaju planske kontrole, uključujući oblikovanje politika i dokumentirane dodjele uloga.

11.3.3 CA-1: zahtijeva definirane uloge za procjenu i autorizaciju.

11.3.4 AC-1: povezuje kontrolu pristupa utemeljenu na ulogama (RBAC) s dodijeljenim odgovornostima upravljanja.

11.4 GDPR EU

11.4.1 Članak 5(2) – Odgovornost: zahtijeva da organizacije mogu dokazati usklađenost putem jasno utvrđenih uloga i odgovornosti.

11.4.2 Članak 32 – Sigurnost obrade: naglašava jasnu dodjelu dužnosti radi zaštite osobnih podataka.

11.5 EU NIS

11.5.1 Članak 21(2)(a): zahtijeva strukture upravljanja koje uključuju formalizirane uloge za upravljanje kibernetičkim rizicima i incidentima.

11.6 EU DORA

11.6.1 Članci 9 i 10: zahtijevaju da financijski subjekti jasno dodijele i nadziru odgovornosti povezane s IKT-om i sigurnošću.

11.7 COBIT 2019

11.7.1 EDM03 – Osigurati optimizaciju rizika: zahtijeva dobro definirane uloge i putove eskalacije za upravljanje sigurnosnim rizikom.

11.7.2 APO13 – Upravljanje sigurnošću: dodjeljuje strateške i operativne sigurnosne dužnosti pojedincima i ulogama.

11.7.3 DSS05 – Upravljanje sigurnosnim uslugama: zahtijeva strukturu i sljedivost odgovornosti za vanjske i interne sigurnosne usluge.