					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P06S					Naziv dokumenta: **Politika upravljanja rizicima**							
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**

Usklađenost sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 do RA-7, PM-9	
EU NIS2	Članak 21(2)(a–d)	
EU DORA	Članak 5	
COBIT 2019	APO12, MEA01	

1. Svrha

1.1 Ova politika definira način na koji organizacija identificira, procjenjuje i upravlja rizicima povezanima s informacijskom sigurnošću, poslovnim operacijama, tehnologijom i uslugama trećih strana.

1.2 Ovom politikom osigurava se da je upravljanje rizicima sastavni dio planiranja, provedbe projekata, odabira dobavljača i odgovora na incidente, u skladu s normama ISO 27001, ISO 31000 i primjenjivim regulatornim zahtjevima.

1.3 Ova politika podupire odlučivanje temeljeno na riziku, zaštitu informacijske imovine i otpornost ključnih poslovnih operacija.

2. Opseg

2.1 Ova se politika primjenjuje na:

2.1.1 sve odjele, sustave i korisnike unutar organizacije

2.1.2 sve informacije, usluge i imovinu kojom se upravlja interno ili putem trećih strana

2.1.3 aktivnosti povezane s upravljanjem rizicima, uključujući preglede projekata, nadogradnje sustava, izdvajanje usluga i usklađivanje s regulatornim zahtjevima

2.2 Obuhvaća sve vrste rizika, uključujući:

2.2.1 prijetnje kibernetičkoj sigurnosti i ranjivosti sustava

2.2.2 operativne poremećaje i prekide usluga

2.2.3 pravnu, regulatornu ili reputacijsku izloženost

2.2.4 rizike povezane s trećim stranama i opskrbnim lancem

2.3 Svi zaposlenici, ugovorni izvođači i pružatelji usluga moraju postupati u skladu s ovom politikom pri identifikaciji ili prijavljivanju rizika.

3. Ciljevi

3.1 Ugraditi jednostavne i ponovljive postupke procjene rizika u redovno poslovanje.

3.2 Identificirati i odrediti prioritete rizika koji mogu utjecati na povjerljivost, cjelovitost, dostupnost ili pravnu usklađenost.

3.3 Dodijeliti vlasništvo i definirati mjere obrade za sve značajne rizike.

3.4 Održavati točan i ažuran registar rizika radi dokazivanja usklađenosti i praćenja rizika.

3.5 Osigurati uključenost uprave u odobravanje tolerancije na rizik i ključnih planova obrade rizika.

4. Uloge i odgovornosti

4.1 Direktor

4.1.1 Utvrđuje apetit za rizik organizacije i odobrava okvir upravljanja rizicima.

4.1.2 Odobrava ključne odluke o obradi rizika i potrebne resurse.

4.1.3 Tromjesečno preispituje najznačajnije rizike s koordinatorom za rizike.

4.2 Koordinator za rizike (ili vlasnik ISMS-a)

4.2.1 Provodi procjene rizika i održava registar rizika.

4.2.2 Osigurava da su ocjenjivanje rizika, vlasništvo i mjere obrade dokumentirani.

4.2.3 Organizira najmanje jedan formalni pregled rizika godišnje.

[... 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 politike

9.1.1 Ovu politiku moraju najmanje jednom godišnje preispitati direktor i koordinator za rizike kako bi se osigurala njezina relevantnost i potpunost.

9.2 Okidači za ažuriranje

9.2.1 Raniji pregled i ažuriranje moraju se provesti ako:

9.2.1.1 značajan incident ili nalaz revizije otkrije nedostatke u kontrolama rizika

9.2.1.2 uvedu se nove poslovne jedinice, tehnologije ili partnerstva

9.2.1.3 promijeni se regulatorni ili ugovorni zahtjev

9.3 Upravljanje verzijama

9.3.1 Sva ažuriranja ove politike moraju biti verzionirana sa sljedećim metapodacima:

9.3.1.1 broj verzije i datum stupanja na snagu

9.3.1.2 sažetak promjena

9.3.1.3 odobrio (direktor)

9.3.1.4 arhivirane prethodne verzije za potrebe revizije

9.4 Komunikacija i podizanje svijesti

9.4.1 Ažurirane verzije politike i ključni planovi obrade rizika moraju se priopćiti obuhvaćenom osoblju. Godišnja obnova osposobljavanja mora uključivati osnovna načela osviještenosti o rizicima.

10. Povezane politike i poveznice

10.1 Ova se politika provodi usklađeno s drugim politikama kako bi se osiguralo sveobuhvatno upravljanje sigurnošću:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: Definira tko je odgovoran za vlasništvo nad rizikom i donošenje odluka.

10.1.2 P5S – Politika upravljanja promjenama: Zahtijeva procjenu rizika prije provedbe tehničkih ili procesnih promjena.

10.1.3 P17S – Politika zaštite podataka i privatnosti: Uređuje regulatorni rizik povezan s postupanjem s osobnim podacima.

10.1.4 P30S – Politika odgovora na incidente: Osigurava da se obrada rizika nastavlja tijekom i nakon sigurnosnih incidenata.

10.1.5 P33S – Politika kontinuiteta poslovanja: Identificira preostale rizike i mjere oporavka za kritične usluge.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – Uspostavlja formalni postupak upravljanja rizicima i planiranja obrade rizika.

11.1.2 Točka 6.1.3 – Zahtijeva da organizacije zadrže dokumentirane planove obrade i odobrenja.

11.2 ISO/IEC 27002

11.2.1 Kontrole 5.4 i 5.25 – Daju smjernice za provedbu vlasništva nad rizikom, određivanja prioriteta i upravljanja životnim ciklusom.

11.3 NIST SP 800-53 Rev. 5

11.3.1 RA-1 do RA-7 – Definiraju procjenu rizika, strategije odgovora, dokumentaciju i mehanizme pregleda.

11.4 PM-9

11.4.1 Zahtijeva dosljedan nadzor organizacijskih rizika na razini uprave.

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(a–d) – Propisuje obvezne kontrole procjene rizika, ublažavanja i upravljanja za ključne i važne subjekte.

11.6 Uredba EU DORA

11.6.1 Članak 5 – Zahtijeva da regulirani subjekti uspostave i održavaju okvir za upravljanje IKT rizicima, uključujući identifikaciju, klasifikaciju i odgovor.

11.7 COBIT 2019

11.7.1 APO12 – Upravljanje rizicima: Integrira rizik u strateško i operativno planiranje.

11.7.2 MEA01 – Praćenje, vrednovanje i ocjenjivanje: Osigurava djelotvornost i usklađenost procesa i aktivnosti upravljanja rizicima.