					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P02					Naslov dokumenta: **Politika upravljanja vlog in odgovornosti**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 5.3; Priloga 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	
Uredba EU GDPR	Členi 5(1)(f), 24, 37	
Direktiva EU NIS2	Člen 21(2)(a)	
Uredba EU DORA	Člen 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Namen

1.1 Ta politika določa model upravljanja ter organizacijske vloge in odgovornosti, potrebne za učinkovito delovanje sistema upravljanja informacijske varnosti (ISMS).

1.2 Določa jasne linije odgovornosti, pooblastila za odločanje in eskalacijske poti, da se informacijska varnost vključi na vseh ravneh organizacije in uskladi s strateškimi poslovnimi cilji.

1.3 Ta politika uvaja zahteve standarda ISO/IEC 27001:2022, klavzule 5.3 in kontrole A.5.2, ter zagotavlja, da so odgovornosti za dejavnosti, povezane z varnostjo, jasno dodeljene, dokumentirane, sporočene in periodično pregledovane.

1.4 Ta politika vzpostavlja tudi podlago za integrirano upravljanje z drugimi področji, kot so obvladovanje tveganj, skladnost, IT-operacije in pravne funkcije.

2. Obseg

2.1 Ta politika velja za vse posameznike in subjekte, vključene v upravljanje, izvajanje in nadzor informacijske varnosti znotraj obsega ISMS. To vključuje:

2.1.1 izvršno vodstvo, najvišje vodstvo in člane upravnega odbora,

2.1.2 vodje ISMS, vodje informacijske varnosti (CISO) in lastnike kontrol,

2.1.3 lastnike procesov in sredstev,

2.1.4 izvajalce in zunanje ponudnike storitev z delegiranimi odgovornostmi na področju varnosti.

2.2 Zajema tako interno izvajane kot zunanje izvajane funkcije (npr. zunanji varnostno-operativni center (SOC), skrbniki oblačne platforme), kadar so vloge upravljanja formalno dodeljene ali pogodbeno opredeljene.

2.3 Politika velja tudi za organizacijske enote, oddelke in projektne skupine, ki upravljajo sredstva, sisteme ali storitve, pomembne za varnost, ali nanje vplivajo.

3. Cilji

3.1 Zagotoviti, da so vloge in odgovornosti na področju informacijske varnosti formalno opredeljene, dodeljene, sporočene in dokumentirane.

3.2 Vzdrževati model upravljanja, ki zagotavlja ločevanje dolžnosti (SoD), preprečuje nasprotje interesov in omogoča eskalacijo nerešenih varnostnih vprašanj.

3.3 Zagotoviti, da sta odgovornost in pooblastilo za sprejemanje varnostnih odločitev razporejena skladno z vplivom na poslovanje in organizacijsko strukturo.

3.4 Vzpostaviti okvir za upravljanje delegiranja, sprememb vlog in pregledov dodeljenih odgovornosti.

3.5 Zainteresiranim stranem, vključno z regulatorji, presojevalci in strankami, zagotoviti potrditev, da se informacijska varnost učinkovito upravlja in da je zagotovljena skladnost z veljavnimi standardi.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Zagotavlja strateški nadzor, dodeljuje vire in zagotavlja usklajenost med cilji ISMS in poslovnimi cilji.

4.1.2 Odobrava ključno dokumentacijo ISMS, vključno s Politiko informacijske varnosti, načrti obravnave tveganj in odločitvami o odpravi revizijskih ugotovitev.

4.1.3 Sodeluje pri vodstvenih pregledih ISMS in eskalira odločitve, ki zahtevajo odobritev na ravni upravnega odbora.

4.1.4 Spodbuja kulturo varnosti in podpira upoštevanje načel varnostnega upravljanja v organizaciji.

4.2 Usmerjevalni odbor za informacijsko varnost (ISSC)

4.2.1 Deluje kot medfunkcijski organ upravljanja za nadzor nad ISMS.

4.2.2 Pregleduje profil tveganj, uspešnost kontrol, ugotovitve presoj in strateške varnostne pobude.

4.2.3 Omogoča usklajevanje med oddelki (npr. IT, pravna služba, človeški viri (HR), tveganja, skladnost, operacije).

4.2.4 Odobrava pragove eskalacije, dodelitev proračuna in spremembe politik, ki zahtevajo prispevek izvršnega vodstva.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Razpored pregledov

9.1.1 Ta politika se mora pregledati najmanj enkrat letno ali ob nastopu naslednjih dogodkov:

9.1.1.1 spremembe organizacijske strukture ali izvršne ekipe,

9.1.1.2 razširitev ali ponovna opredelitev obsega ISMS,

9.1.1.3 regulatorne spremembe, ki vplivajo na dodelitev vlog ali nadzor,

9.1.1.4 pomembne ugotovitve presoje ali incidenti, povezani z odpovedjo upravljanja.

9.2 Postopek pregleda in odobritve

9.2.1 Vodja ISMS mora začeti in voditi postopek pregleda, vključno z zbiranjem prispevkov zainteresiranih strani in povratnih informacij iz presoj.

9.2.2 Predlagane posodobitve mora pregledati ISSC, formalno pa jih mora odobriti najvišje vodstvo.

9.2.3 Vsaka različica mora biti evidentirana v registru dokumentov ISMS in mora vključevati naslednje metapodatke:

9.2.3.1 identifikator in naslov politike,

9.2.3.2 številko različice in povzetek sprememb,

9.2.3.3 datum začetka veljavnosti in datum naslednjega pregleda,

9.2.3.4 lastnika politike in odobritelja,

9.2.3.5 raven klasifikacije dokumenta,

9.2.3.6 zgodovino hrambe in arhiviranja.

10. Povezane politike in povezave

10.1 To politiko je treba razlagati skupaj z naslednjimi politikami:

10.1.1 P1 – Politika informacijske varnosti: določa celovit program informacijske varnosti in opredeljuje odgovornosti vodstva za potrditev politike in strateški nadzor.

10.1.2 P5 – Politika upravljanja sprememb: zagotavlja, da za spremembe struktur upravljanja, vlog ali odgovornosti veljata dokumentirana odobritev in pregled tveganj.

10.1.3 P6 – Politika obvladovanja tveganj: prepoznava in obravnava tveganja upravljanja, ki izhajajo iz nasprotujočih si vlog, nedodeljenih nalog ali pomanjkljive eskalacije.

10.1.4 P7 – Politika uvajanja in prenehanja: zagotavlja izvajanje procesov dodelitve kontrol in preklica v okviru sprememb v življenjskem ciklu zaposlenih.

10.1.5 P33 – Politika spremljanja presoj in skladnosti: podpira neodvisen pregled učinkovitosti upravljanja in zahteva korektivne ukrepe ob neskladnosti.

10.2 Te politike skupaj podpirajo enoten in izvršljiv okvir upravljanja ISMS.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z globalno priznanimi standardi in okviri za upravljanje informacijske varnosti ter odgovornosti za vloge. Zagotavlja sledljivost do regulatornih in certifikacijskih zahtev ter podpira utemeljeno strukturo ISMS.

11.2 ISO/IEC 27001

11.2.1 Klavzula 5.3 – Organizacijske vloge, odgovornosti in pooblastila: ta politika izpolnjuje zahtevo, da so vloge, pomembne za informacijsko varnost, jasno dodeljene, sporočene in dokumentirane.

11.2.2 Klavzula 9.3 – Vodstveni pregled: ta politika zagotavlja izvršni nadzor nad vlogami ISMS in upravljanjem prek četrtletnih in letnih pregledov.

11.2.3 Priloga A, kontrola 5.2 – Vloge in odgovornosti na področju informacijske varnosti: opredeljuje vloge na tehnični, operativni in strateški ravni, da se zagotovijo ločevanje dolžnosti (SoD), lastništvo tveganj in sledljiva odgovornost.

11.3 ISO/IEC 27002:2022 – Kontrola 5

11.3.1 Podaja smernice za izvajanje dodeljevanja odgovornosti za informacijsko varnost v organizaciji. Ta politika te smernice prevzema z opredelitvijo vrst vlog, pravil delegiranja, postopkov eskalacije in mehanizmov pregledovanja.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1 do PL-4: določajo potrebo po formalni planski dokumentaciji, vključno s politikami, ki opredeljujejo upravljanje in dodeljujejo varnostne odgovornosti.

11.4.2 PM-1 (načrt programa informacijske varnosti) in PM-2 (višji uradnik za informacijsko varnost): v tej politiki sta odražena z dodelitvijo vloge CISO/vodje ISMS in formalnih vlog upravljanja.

11.4.3 PM-5 do PM-13: ta politika izpolnjuje zahteve glede dokumentiranja vlog, vlog tveganj na ravni organizacije, nadzora upravljanja konfiguracij in integracije s poslovnimi funkcijami.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 5(1)(f): zahteva, da so osebni podatki zaščiteni pred nepooblaščeno ali nezakonito obdelavo. Ta politika zagotavlja, da so posamezniki, odgovorni za varstvo podatkov, jasno določeni in nadzorovani.

11.5.2 Člen 24: zahteva ustrezne organizacijske ukrepe, vključno s strukturami upravljanja.

11.5.3 Člen 37: zahteva imenovanje pooblaščene osebe za varstvo podatkov (DPO), kar mora biti odraženo v okviru upravljanja organizacije in registru odgovornosti.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Člen 21(2)(a): določa, da morajo subjekti izvajati politike glede analize tveganj in varnosti informacijskih sistemov, vključno z odgovornostmi, prilagojenimi vlogam. Ta politika opredeljuje takšne vloge in njihove mehanizme upravljanja.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Člen 5 – Okvir upravljanja in notranjih kontrol: zahteva formalno dodelitev odgovornosti za upravljanje tveganj IKT, vlog odločanja in kanalov poročanja. Ta politika predstavlja podlago za upravljanje vlog, povezanih z varnostjo, v okoljih IKT.

11.8 COBIT 2019

11.8.1 EDM01 – Vzpostavljen okvir upravljanja: ta politika zagotavlja, da ima ISMS jasno opredeljeno strukturo upravljanja, usklajeno s potrebami organizacije.

11.8.2 EDM02 – Zagotovljeno ustvarjanje koristi: usklajuje varnostne dejavnosti na podlagi vlog s strateškimi in operativnimi cilji ter zagotavlja odgovornost in merljive rezultate.

11.8.3 APO01 – Upravljan okvir upravljanja I&T in APO12 – Upravljano tveganje: ta politika podpira strukturirano upravljanje vlog informacijske varnosti v širšem okviru upravljanja IT in tveganj.

11.8.4 MEA01 – Spremljanje, vrednotenje in ocenjevanje uspešnosti: vključuje mehanizme pregledovanja za preverjanje, da so vloge upravljanja učinkovite, aktualne in se izvajajo.