					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P02S					Naslov dokumenta: **Politika vlog in odgovornosti pri upravljanju**							
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	
ISO/IEC 27002:2022	Kontrole: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev. 5	PM-1, PL-1, PL-4, CA-1, AC-1	
Uredba EU GDPR	Člena 5(2), 32	

1. Namen

1.1 Ta politika določa, kako se v organizaciji dodeljujejo, delegirajo in upravljajo odgovornosti pri upravljanju informacijske varnosti, da se zagotovi popolna skladnost z ISO/IEC 27001:2022 in drugimi regulativnimi obveznostmi.

1.2 Zagotavlja odgovornost na vseh ravneh ter podpira operativno učinkovitost z jasno opredelitvijo odgovornosti za vsako funkcijo, povezano z varnostjo.

1.3 Ta politika izboljšuje pripravljenost na presojo in krepi zaupanje strank z dokazovanjem formaliziranega upravljanja informacijske varnosti, tudi v organizacijah z omejenimi tehničnimi viri ali zunanjim izvajanjem IT-storitev.

2. Področje uporabe

2.1 Ta politika velja za vse posameznike, ki upravljajo organizacijske sisteme ali podatke, vključno z:

2.1.1 poslovnimi lastniki in generalnim direktorjem

2.1.2 zaposlenimi in pogodbenimi izvajalci

2.1.3 zunanjimi ponudniki IT-storitev ali svetovalci

2.2 Zajema vse sisteme, okolja in storitve, ki se uporabljajo za obdelavo, prenos ali hrambo poslovnih informacij ali informacij strank, vključno z:

2.2.1 pisarniško IT-infrastrukturo in napravami za delo na daljavo

2.2.2 platformami v oblaku in storitvami elektronske pošte

2.2.3 fizično dokumentacijo in skupnimi diski

2.3 Obseg vključuje notranje in zunanje izvajane dejavnosti, povezane z upravljanjem informacijske varnosti.

3. Cilji

3.1 Vzpostaviti jasno odgovornost za vse naloge, povezane z varnostjo, vključno z upravljanjem politik, nadzorom dostopa, obravnavo incidentov in spremljanjem.

3.2 Omogočiti učinkovito ločevanje dolžnosti (SoD) za zmanjšanje nasprotja interesov ali tveganja goljufij.

3.3 Zagotoviti, da so varnostne naloge in vloge jasno dokumentirane ter se redno pregledujejo.

3.4 Omogočiti informirano odločanje, eskalacijo in nadzor nad IT- in varnostnimi tveganji.

3.5 Podpreti certificiranje po ISO/IEC 27001:2022 ter okrepiti zaupanje strank, partnerjev in presojevalcev.

4. Vloge in odgovornosti

4.1 Generalni direktor / poslovni lastnik

4.1.1 Je v celoti odgovoren za uvedbo in nadzor izvajanja te politike.

4.1.2 Odobrava vse varnostne vloge, odgovornosti in odločitve o delegiranju.

4.1.3 Spremlja skladnost ter sprejema končne odločitve o izjemah od politike in eskalacijah.

4.2 Imenovani koordinator za informacijsko varnost (če je določen)

4.2.1 To je lahko član osebja ali zaupanja vreden svetovalec.

4.2.2 To vlogo lahko v mikropodjetjih prevzame generalni direktor ali zunanji ponudnik.

4.2.3 Pomaga pri vsakodnevnem izvajanju nadzora dostopa, odzivanju na incidente in izvajanju osnovnih tehničnih varnostnih nalog.

4.2.4 O vseh varnostnih vprašanjih ali tveganjih poroča neposredno generalnemu direktorju.

[... 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 Letni pregled

9.1.1 Generalni direktor mora to politiko pregledati vsakih 12 mesecev, da se zagotovi njena stalna usklajenost s pravnimi obveznostmi, operativnimi potrebami in zahtevami za certificiranje po ISO/IEC 27001.

9.2 Vmesni pregledi

9.2.1 Pregledi se morajo izvesti tudi, kadar:

9.2.1.1 pride do večjih organizacijskih sprememb

9.2.1.2 se uvede nov ponudnik

9.2.1.3 pride do resnega varnostnega incidenta

9.2.1.4 se posodobijo predpisi, kot so Uredba EU GDPR, Direktiva EU NIS2 ali Uredba EU DORA

9.3 Upravljanje različic in dokumentacija

9.3.1 Vsi pregledi morajo vključevati:

9.3.1.1 datum pregleda

9.3.1.2 povzetek vseh sprememb

9.3.1.3 podpis ali dokumentirano odobritev generalnega direktorja

9.3.1.4 arhivirane predhodne različice za potrebe revizijske sledi

9.4 Sporočanje sprememb

9.4.1 Vse posodobitve politike morajo biti nemudoma sporočene zaposlenim in ponudnikom po e-pošti, prek notranjih portalov ali z uradnimi obvestili.

10. Povezane politike in povezave

10.1 To politiko je treba za popolno učinkovitost izvajati skupaj z naslednjimi politikami SME:

10.1.1 P4S – Politika nadzora dostopa: določa, kako se dostop dodeljuje, upravlja in preklicuje, neposredno v povezavi z dodeljenimi vlogami in nadzorom.

10.1.2 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: krepi odgovornosti in pričakovanja, prilagojena vlogam.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: opredeljuje pravne obveznosti po GDPR, ki so dodeljene vlogam, določenim v tej politiki upravljanja.

10.1.4 P30S – Politika odzivanja na incidente: zahteva jasno opredeljene odgovornosti za poročanje, eskalacijo in razreševanje incidentov.

10.2 Te politike skupaj omogočajo dosledno izvajanje, notranjo odgovornost in zunanjo skladnost.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 5.3 – Organizacijske vloge, odgovornosti in pooblastila: zahteva jasno dodeljene vloge in podporo najvišjega vodstva.

11.2 ISO/IEC 27002

11.2.1 Kontrole 5.2–5.4: zahtevajo jasno dokumentiranje vlog informacijske varnosti, ločevanje dolžnosti in vodstveni nadzor.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PM-1: vzpostavlja krovni program informacijske varnosti z določenimi odgovornostmi.

11.3.2 PL-1 do PL-4: zahtevajo planske kontrole, vključno z oblikovanjem politik in dokumentiranimi dodelitvami vlog.

11.3.3 CA-1: zahteva opredeljene vloge za presojo in odobritev.

11.3.4 AC-1: povezuje nadzor dostopa na podlagi vlog z dodeljenimi odgovornostmi upravljanja.

11.4 Uredba EU GDPR

11.4.1 Člen 5(2) – Odgovornost: zahteva, da organizacije dokazujejo skladnost z vlogami in odgovornostmi.

11.4.2 Člen 32 – Varnost obdelave: poudarja jasno dodelitev nalog za varovanje osebnih podatkov.

11.5 Direktiva EU NIS

11.5.1 Člen 21(2)(a): zahteva strukture upravljanja, ki vključujejo formalizirane vloge za obvladovanje kibernetskih tveganj in incidentov.

11.6 Uredba EU DORA

11.6.1 Člena 9 in 10: zahtevata, da finančni subjekti jasno dodelijo in nadzorujejo odgovornosti, povezane z IKT in varnostjo.

11.7 COBIT 2019

11.7.1 EDM03 – Zagotavljanje optimizacije tveganj: zahteva jasno opredeljene vloge in eskalacijske poti za obvladovanje varnostnih tveganj.

11.7.2 APO13 – Upravljanje varnosti: dodeljuje strateške in operativne varnostne naloge posameznikom in vlogam.

11.7.3 DSS05 – Upravljanje varnostnih storitev: zahteva strukturo in sledljivost odgovornosti za zunanje in notranje varnostne storitve.