					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P01S					Naslov dokumenta: **Politika informacijske varnosti**							
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	Klavzule 5.1, 5.2, 5.3, 6.1, 6.2, 8	Določa zavezanost vodstva, zahteve glede politike, dodelitev vlog, oceno tveganj in operativni nadzor
ISO/IEC 27002:2022	Kontrole 5.1–5	Določa pripravo dokumentiranih politik informacijske varnosti, dodelitev vlog, ločevanje dolžnosti in odgovornosti vodstva
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Določa zahteve za načrt programa informacijske varnosti, politiko varnostnega načrtovanja, presojo/odobritev in nadzor dostopa
EU GDPR (2016/679)	Člen 5(2), člen 32	Določa načelo odgovornosti in ukrepe za varnost obdelave, zlasti glede dokumentiranih vlog
Direktiva EU NIS2 (2022/2555)	Člen 21(2)(a)	Zahteva ukrepe za obvladovanje tveganj ter opredeljene vloge in odgovornosti za kibernetska tveganja
Uredba EU DORA (2022/2554)	Člen 9, člen 10	Zahteva dodelitev vlog za upravljanje IKT-tveganj in neprekinjeno poslovanje
COBIT 2019	EDM03, APO13, DSS05	Določa optimizacijo tveganj, upravljanje varnosti in upravljanje varnostnih storitev z jasno dodelitvijo vlog

1. Namen

1.1 Ta politika izkazuje zavezanost organizacije varovanju informacij strank in poslovnih informacij z jasno opredelitvijo odgovornosti ter praktičnih varnostnih ukrepov, primernih za organizacije brez namenskih IT-ekip.

1.2 Zagotavlja, da vsi zaposleni, pogodbeni izvajalci in ponudniki storitev upoštevajo zavezujoča pravila, s čimer se omogoča popolna skladnost z zahtevami certifikacije ISO/IEC 27001.

1.3 Ta politika organizaciji omogoča krepitev zaupanja strank, saj jasno izkazuje, kako so njihove informacije zaščitene z opredeljenimi odgovornostmi, strukturiranimi procesi in jasno odgovornostjo.

2. Obseg

2.1 Ta politika velja za vse posameznike, ki dostopajo do podatkov in sistemov organizacije ali z njimi upravljajo, vključno z:

2.1.1 lastniki podjetja in glavnim izvršnim direktorjem

2.1.2 zaposlenimi, pogodbenimi izvajalci in praktikanti

2.1.3 zunanjimi ponudniki IT-storitev ali svetovalci

2.2 Zajema vse vrste informacij, sistemov in storitev, vključno z:

2.2.1 poslovnimi evidencami, podatki o strankah, gesli in elektronsko pošto

2.2.2 IT-opremo, kot so prenosni računalniki in telefoni

2.2.3 storitvami v oblaku, ki se uporabljajo za shranjevanje datotek, komunikacijo ali finance

2.2.4 fizičnimi dokumenti, shranjenimi na lokacijah organizacije

2.3 Politika velja v vseh delovnih okoljih – v pisarni, pri delu na daljavo in v okolju v oblaku – ter zajema vse naprave in programsko opremo, ki se uporabljajo za obdelavo ali shranjevanje poslovnih informacij.

3. Cilji

3.1 Jasna dodelitev odgovornosti: zagotoviti, da je za informacijsko varnost vedno določena odgovorna oseba. To je praviloma glavni izvršni direktor ali oseba, ki jo ta formalno določi.

3.2 Varovanje informacij strank in poslovnih informacij: zagotoviti zanesljive in dosledne zaščitne ukrepe za preprečevanje zlorabe, izgube ali kraje občutljivih podatkov, vključno s podatki o strankah in finančnimi evidencami.

3.3 Podpora certifikaciji ISO/IEC 27001: organizaciji omogočiti dokazovanje popolne skladnosti z zahtevami ISO/IEC 27001 ter pripravljenost na presojo in certifikacijo brez potrebe po kompleksni infrastrukturi.

3.4 Vključitev varnosti v poslovanje: vključiti informacijsko varnost v vsakodnevne naloge in odločitve v celotni organizaciji.

3.5 Krepitev varnostne ozaveščenosti in kulture: zagotoviti, da vsak zaposleni razume in upošteva varnostne prakse, kot so uporaba močnih gesel in poročanje o sumljivih dejavnostih.

4. Vloge in odgovornosti

4.1 Glavni izvršni direktor ali lastnik podjetja

4.1.1 Nosi celotno odgovornost za informacijsko varnost.

4.1.2 Odobri in vzdržuje to politiko.

4.1.3 Zagotovi, da se vse ključne varnostne naloge izvajajo neposredno ali da so pisno delegirane.

4.1.4 Preverja, da se vse delegirane varnostne naloge (kot so upravljanje dostopa ali odzivanje na incidente) izvajajo učinkovito.

4.1.5 Je privzeta kontaktna točka za vse notranje in zunanje varnostne zadeve, vključno s presojami in poizvedbami strank.

4.1.6 Med letnim pregledom spremlja napredek glede na te cilje. Kjer je to mogoče, morajo biti cilji merljivi (npr. odstotek usposobljenega osebja, število prijavljenih incidentov) in se morajo pregledati na podlagi varnostnih ugotovitev in sprememb tveganj.

4.2 Določeni zaposleni (če je ustrezno)

4.2.1 Lahko pomaga glavnemu izvršnemu direktorju pri vsakodnevnih nalogah, kot so ustvarjanje uporabniških računov, ukinitev dostopa odhajajočim zaposlenim ali usklajevanje s ponudnikom IT.

4.2.2 Mora biti uradno določen ter imeti zadostna pooblastila in orodja za izvajanje nalog.

4.2.3 O vseh vprašanjih poroča glavnemu izvršnemu 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 To politiko mora glavni izvršni direktor (GID) pregledati najmanj enkrat letno, da zagotovi stalno skladnost z zahtevami certifikacije ISO/IEC 27001, regulativnimi spremembami (kot so GDPR, NIS2 in DORA) ter spreminjajočimi se poslovnimi potrebami.

9.2 Vmesni pregledi

9.2.1 Dodatni pregledi se morajo izvesti ob vseh pomembnih spremembah, kot so:

9.2.1.1 večji varnostni incidenti ali kršitve

9.2.1.2 uvedba novih poslovnih procesov ali tehnologij (npr. nova programska oprema, platforme za delo na daljavo ali storitve v oblaku)

9.2.1.3 spremembe pravnih ali regulativnih zahtev, ki vplivajo na ravnanje z informacijami

9.3 Dokumentiranje sprememb

9.3.1 Vsi pregledi politike in spremembe morajo biti formalno dokumentirani, z jasno navedenim datumom, naravo sprememb in odobritvijo GID.

9.3.2 Zgodovinska evidenca različic politike se mora varno hraniti za dokazovanje razvoja politike in skladnosti med presojami.

9.4 Obveščanje o posodobitvah

9.4.1 O vseh spremembah te politike je treba nemudoma obvestiti vse zaposlene, pogodbene izvajalce in relevantne tretje osebe.

9.4.2 Posodobljene različice politike morajo biti lahko dostopne vsem zadevnim osebam (npr. v elektronski obliki v skupnem delovnem prostoru ali fizično objavljene na delovnem mestu).

10. Povezane politike in povezave

10.1 Ta politika je tesno povezana z drugimi politikami iz sklopa SME v organizaciji, zlasti z:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: pojasnjuje dodelitev varnostnih nalog in odgovornosti.

10.1.2 P4S – Politika nadzora dostopa: opredeljuje varno upravljanje dostopa do informacij podjetja.

10.1.3 P8S – Politika ozaveščanja in usposabljanja na področju informacijske varnosti: določa ključne smernice za usposabljanje in ozaveščanje osebja.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: zagotavlja skladnost z GDPR in drugimi predpisi s področja varstva podatkov.

10.1.5 P30S – Politika odzivanja na incidente: opisuje podrobne ukrepe, potrebne za odziv na varnostne incidente.

10.2 Te povezane politike zagotavljajo jasne operativne usmeritve in jih je treba izvajati skupaj za doseganje popolne skladnosti z zahtevami certifikacije ISO/IEC 27001.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 5.1 – Vodenje in zavezanost: zahteva zavezanost najvišjega vodstva in odgovornost za učinkovitost informacijske varnosti v organizaciji.

11.1.2 Klavzula 5.2 – Politika informacijske varnosti: zahteva jasne, dokumentirane politike, usklajene s strategijo organizacije in zahtevami skladnosti.

11.1.3 Klavzula 5.3 – Organizacijske vloge in odgovornosti: določa jasno dodelitev odgovornosti za informacijsko varnost v celotni organizaciji, kar je bistveno za učinkovito upravljanje in skladnost pri presojah.

11.1.4 Klavzula 6.1 – Ukrepi za obravnavo tveganj in priložnosti: določa sistematično prepoznavanje, ocenjevanje in obravnavo tveganj informacijske varnosti.

11.1.5 Klavzula 8.1 – Operativno načrtovanje in nadzor: zahteva, da organizacija načrtuje in izvaja procese, potrebne za doseganje ciljev informacijske varnosti, ter učinkovito upravlja povezana tveganja.

11.2 ISO/IEC 27002:2022 Kontrole 5.1–5

11.2.1 Priloga A Kontrola 5.1 – Politike informacijske varnosti: določa pripravo in sporočanje dokumentiranih politik informacijske varnosti.

11.2.2 Priloga A Kontrola 5.2 – Vloge informacijske varnosti: pojasnjuje in formalno dodeljuje vloge in odgovornosti na področju informacijske varnosti relevantnim deležnikom.

11.2.3 Priloga A Kontrola 5.3 – Ločevanje dolžnosti (SoD): zahteva jasno ločevanje dolžnosti za zmanjšanje nasprotij interesov in tveganj prevar pri upravljanju občutljivih informacij.

11.2.4 Priloga A Kontrola 5.4 – Odgovornosti vodstva: zahteva, da vodstvo izkazuje zavezanost informacijski varnosti z aktivnim nadzorom in dodeljevanjem virov.

11.2.5 Krepi potrebo po jasno dokumentiranih politikah informacijske varnosti, vlogah, odgovornostih in strukturah upravljanja ter zagotavlja dosledno upravljanje in revizijsko sled v celotni organizaciji.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Načrt programa informacijske varnosti: zahteva dokumentirane strategije in politike upravljanja informacijske varnosti ter zagotavlja okvir za dosledno izvajanje in upravljanje.

11.3.2 PL-1 – Politika varnostnega načrtovanja: zahteva organizacijsko politiko varnostnega načrtovanja za usmerjanje varnega delovanja in strateške usklajenosti dejavnosti informacijske varnosti.

11.3.3 CA-1 – Politika presoje in odobritve varnosti: zahteva jasno opredeljene vloge za presojo in odobritev za zagotavljanje stalne učinkovitosti in skladnosti z zahtevami informacijske varnosti.

11.3.4 AC-1 – Politika nadzora dostopa: zahteva, da organizacije jasno opredelijo, dokumentirajo in uveljavijo prakse ter odgovornosti upravljanja dostopa.

11.4 EU GDPR (2016/679)

11.4.1 Člen 5(2) – Načelo odgovornosti: zahteva, da organizacije dokazujejo skladnost z načeli varstva podatkov, vključno z dokumentiranimi vlogami in politikami za odgovornosti na področju varstva podatkov.

11.4.2 Člen 32 – Varnost obdelave: zahteva izvajanje ustreznih tehničnih in organizacijskih ukrepov, vključno z jasno določenimi varnostnimi odgovornostmi, za zaščito osebnih podatkov pred kršitvami in nepooblaščenim dostopom.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a) – Ukrepi za obvladovanje tveganj: zahteva jasne ureditve upravljanja, vključno z opredeljenimi vlogami in odgovornostmi za informacijsko varnost, ki so bistvene za učinkovito obvladovanje kibernetskih tveganj.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – Upravljanje IKT-tveganj: zahteva, da organizacije jasno dodelijo vloge in odgovornosti, povezane z upravljanjem IKT-tveganj, s čimer krepijo odpornost in pripravljenost za neprekinjeno poslovanje.

11.6.2 Člen 10 – Neprekinjeno poslovanje IKT: zahteva jasno odgovornost in strukturirane vloge za vzdrževanje odpornosti in neprekinjenega delovanja IKT ter zagotavlja, da se organizacije lahko zanesljivo odzovejo na motnje.

11.7 COBIT 2019

11.7.1 EDM03 – Zagotavljanje optimizacije tveganj: poudarja jasno opredeljeno odgovornost in vloge pri upravljanju organizacijskih tveganj ter zagotavlja močno upravljanje in učinkovit nadzor tveganj informacijske varnosti.

11.7.2 APO13 – Upravljanje varnosti: zahteva, da organizacije jasno vzpostavijo in sporočajo odgovornosti za upravljanje varnosti ter zagotovijo usklajenost s poslovnimi cilji in regulativnimi zahtevami.

11.7.3 DSS05 – Upravljanje varnostnih storitev: zahteva strukturirane vloge in jasno določene odgovornosti pri upravljanju varnostnih storitev, kar omogoča dosledno izvajanje in preverjanje skladnosti.