					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P06S					Naslov dokumenta: **Politika obvladovanja tveganj**							
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	Klavzuli 6.1, 6.1.3	
ISO/IEC 27002:2022	Kontroli 5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 do RA-7, PM-9	
Direktiva EU NIS2	Člen 21(2)(a–d)	
Uredba EU DORA	Člen 5	
COBIT 2019	APO12, MEA01 (nadzor, vrednotenje in ocenjevanje)	

1. Namen

1.1 Ta politika določa, kako organizacija prepoznava, ocenjuje in obvladuje tveganja, povezana z informacijsko varnostjo, delovanjem, tehnologijo in storitvami tretjih oseb.

1.2 Zagotavlja, da je proces obvladovanja tveganj sestavni del načrtovanja, izvajanja projektov, izbire dobaviteljev in odzivanja na incidente, v skladu z ISO 27001, ISO 31000 in regulatornimi zahtevami.

1.3 Politika podpira odločanje na podlagi tveganj, varovanje informacijskih sredstev in odpornost ključnih poslovnih dejavnosti.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse oddelke, sisteme in uporabnike v organizaciji;

2.1.2 vse informacije, storitve in sredstva, ki se upravljajo interno ali prek tretjih oseb;

2.1.3 dejavnosti, povezane s tveganji, vključno s pregledi projektov, nadgradnjami sistemov, zunanjim izvajanjem in skladnostjo s predpisi.

2.2 Vključuje vse vrste tveganj, kot so:

2.2.1 kibernetske grožnje in ranljivosti sistemov;

2.2.2 operativne motnje in izpadi storitev;

2.2.3 pravna tveganja, tveganja neskladnosti ali škoda za ugled;

2.2.4 tveganja tretjih oseb in tveganja v dobavni verigi.

2.3 Vsi zaposleni, pogodbeni izvajalci in ponudniki storitev morajo pri prepoznavanju ali poročanju o tveganjih ravnati v skladu s to politiko.

3. Cilji

3.1 V redno poslovanje vključiti enostavne in ponovljive postopke ocenjevanja tveganj.

3.2 Prepoznati in prednostno obravnavati tveganja, ki bi lahko vplivala na zaupnost, celovitost in razpoložljivost (CIA) ali na pravno skladnost.

3.3 Za vsa pomembna tveganja določiti lastništvo in opredeliti ukrepe obravnave.

3.4 Vzdrževati natančen in posodobljen register tveganj za podporo revizijski pripravljenosti in sledljivosti tveganj.

3.5 Zagotoviti vključenost vodstva pri odobritvi apetita po tveganju in ključnih načrtov obravnave tveganj.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Določi apetit po tveganju organizacije in potrdi okvir obvladovanja tveganj.

4.1.2 Odobri ključne odločitve glede obravnave tveganj in potrebne vire.

4.1.3 Četrtletno pregleda najpomembnejša tveganja skupaj s koordinatorjem za tveganja.

4.2 Koordinator za tveganja (ali lastnik ISMS)

4.2.1 Usmerja ocenjevanje tveganj in vzdržuje register tveganj.

4.2.2 Zagotovi, da so ocenjevanje tveganj, lastništvo in ukrepi obravnave ustrezno dokumentirani.

4.2.3 Organizira najmanj en formalni pregled tveganj letno.

[... 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 politike

9.1.1 To politiko morata generalni direktor in koordinator za tveganja pregledati najmanj enkrat letno, da se zagotovi njena ustreznost in popolnost.

9.2 Sprožilci za posodobitev

9.2.1 Predčasen pregled in posodobitev se morata izvesti, če:

9.2.1.1 večji incident ali ugotovitev presoje razkrije vrzeli pri obvladovanju tveganj;

9.2.1.2 se uvedejo nove poslovne enote, tehnologije ali partnerstva;

9.2.1.3 se spremeni regulatorna ali pogodbena zahteva.

9.3 Upravljanje različic

9.3.1 Vse posodobitve te politike morajo biti vodene z različicami z naslednjimi metapodatki:

9.3.1.1 številka različice in datum začetka veljavnosti;

9.3.1.2 povzetek sprememb;

9.3.1.3 odobritelj (generalni direktor);

9.3.1.4 arhivirane predhodne različice za potrebe revizije.

9.4 Komunikacija in ozaveščanje

9.4.1 Posodobljene različice politike in ključni načrti obravnave tveganj morajo biti sporočeni zadevnemu osebju. Letno usposabljanje za ozaveščanje mora vključevati temeljna načela zavedanja o tveganjih.

10. Povezane politike in povezave

10.1 Ta politika deluje usklajeno z več drugimi politikami za zagotovitev celovitega upravljanja varnosti:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa, kdo je odgovoren za lastništvo tveganj in sprejemanje odločitev.

10.1.2 P5S – Politika upravljanja sprememb: zahteva oceno tveganja pred uvedbo tehničnih ali procesnih sprememb.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: obravnava regulatorna tveganja, povezana z obdelavo osebnih podatkov.

10.1.4 P30S – Politika odzivanja na incidente: zagotavlja, da se obravnava tveganj nadaljuje med varnostnimi incidenti in po njih.

10.1.5 P33S – Politika neprekinjenega poslovanja: opredeljuje preostala tveganja in ukrepe za obnovitev kritičnih storitev.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:

11.1.1 Klavzula 6.1 – določa formalni proces obvladovanja tveganj in načrtovanje obravnave tveganj.

11.1.2 Klavzula 6.1.3 – zahteva, da organizacije hranijo dokumentirane načrte obravnave in odobritve.

11.2 ISO/IEC 27002:

11.2.1 Kontroli 5.4 in 5.25 – podajata smernice za izvajanje glede lastništva tveganj, določanja prioritet in upravljanja življenjskega cikla.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 do RA-7 – opredeljujejo ocenjevanje tveganj, strategije odzivanja, dokumentiranje in mehanizme pregledovanja.

11.4 PM-9 – zahteva dosleden nadzor organizacijskih tveganj na ravni vodstva.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(a–d) – nalaga obvezne kontrole za ocenjevanje tveganj, zmanjševanje tveganj in upravljanje pri bistvenih in pomembnih subjektih.

11.6 Uredba EU DORA

11.6.1 Člen 5 – zahteva, da regulirani subjekti opredelijo in upravljajo okvire za obvladovanje IKT-tveganj, vključno s prepoznavanjem, razvrščanjem in odzivanjem.

11.7 COBIT 2019

11.7.1 APO12 – Upravljanje tveganj: vključuje tveganja v strateško in operativno načrtovanje.

11.7.2 MEA01 – Nadzor, vrednotenje in ocenjevanje: zagotavlja učinkovitost in skladnost procesov ter ukrepov za obvladovanje tveganj.