					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P06					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	Klavzule 6.1, 8.32, 10	Jedro prepoznavanja in obvladovanja tveganj, vključitev v upravljanje sprememb, nenehno izboljševanje
ISO/IEC 27005:2024	Celotna metodologija življenjskega cikla tveganj	Celovit proces obvladovanja tveganj v skladu s standardom
ISO 31000:2018	Načela in okvir za obvladovanje tveganj	Načela obvladovanja tveganj, sprejeta v okviru organizacije
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Smernice in struktura za ocenjevanje tveganj, večnivojsko upravljanje tveganj
Uredba EU GDPR	Členi 24, 25, 32	Procesi in kontrole za tveganja na področju varstva osebnih podatkov
Direktiva EU NIS2	Člen 21(2)(a–d)	Obveznosti glede ocenjevanja tveganj in varnosti
Uredba EU DORA	Člena 5, 6	Upravljanje IKT-tveganj in operativna odpornost
COBIT 2019	APO12, MEA	Struktura obvladovanja tveganj in nadzora

1. Namen

1.1 Ta politika vzpostavlja enoten in formaliziran okvir za prepoznavanje, analizo, vrednotenje, obravnavo, spremljanje in pregled tveganj informacijske varnosti v celotni organizaciji.

1.2 Zagotavlja dosledno uporabo načel, temelječih na tveganjih, ki varujejo zaupnost, celovitost in razpoložljivost informacijskih sredstev, v skladu z ISO/IEC 27001:2022, klavzulo 6.1, in ISO 31000:2018.

1.3 Politika vključuje obvladovanje tveganj informacijske varnosti v procese odločanja organizacije z namenom doseganja notranjih strateških ciljev in izpolnjevanja zunanjih regulativnih zahtev.

2. Področje uporabe

2.1 Ta politika velja za vse organizacijske enote, poslovne procese, sisteme, osebje in sodelovanja s tretjimi osebami, ki so vključeni v ravnanje z informacijskimi sredstvi, njihov razvoj, hrambo ali upravljanje.

2.2 Obseg vključuje fizična, digitalna in v oblaku gostovana sredstva, vključno s strukturiranimi in nestrukturiranimi podatki, aplikacijami, infrastrukturo, omrežji in storitvami.

2.3 Zajema tveganja informacijske varnosti na strateški, operativni, projektni in tehnični ravni ter je obvezna za vse zaposlene, pogodbene izvajalce in ponudnike storitev, vključene v dejavnosti ISMS.

2.4 Obvladovanje tveganj se mora uporabljati v naslednjih primerih:

2.4.1 uvedba novega projekta ali sistema

2.4.1.1 pomembne spremembe (npr. arhitekture, lastništva, procesov)

2.4.1.2 vključevanje dobaviteljev in dogovori s tretjimi osebami

2.4.1.3 odziv na incidente in pregledi po incidentu

2.4.1.4 periodični organizacijski pregledi tveganj ali revizije

3. Cilji

3.1 Vzpostaviti in operativno izvajati ponovljiv proces obvladovanja tveganj na ravni celotne organizacije, ki temelji na metodologijah ISO/IEC 27005 in ISO 31000.

3.2 Zagotoviti, da so tveganja prepoznana, analizirana, ovrednotena in obravnavana s strukturiranimi in sledljivimi metodami, vključno z dodelitvijo lastništva tveganj in povezavami s kontrolami.

3.3 Vzdrževati centraliziran register tveganj in načrt obravnave tveganj pod nadzorom različic, ki odražata trenutno stanje tveganj, pokritost s kontrolami in napredek pri zmanjševanju tveganj.

3.4 Uskladiti odločitve o tveganjih z dokumentiranim apetitom po tveganju in ravnmi tolerance do tveganja ter omogočiti informirano vodstveno odločanje glede sprejema tveganja, zmanjševanja tveganj, prenosa ali izogibanja.

3.5 Neprekinjeno spremljati trende tveganj in zagotavljati učinkovitost obravnave tveganj ter omogočati proaktivne prilagoditve na podlagi razvoja groženj ali poslovnih sprememb.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo / upravni odbor

4.1.1 Odobri okvir obvladovanja tveganj ter določi sprejemljiv apetit po tveganju in pragove tolerance do tveganja.

4.1.2 Odobri strategije obravnave tveganj za preostala tveganja, ki presegajo toleranco.

4.1.3 Dodeli vire in izvaja nadzor za učinkovito delovanje programa obvladovanja tveganj.

4.2 Vodja ISMS / pooblaščenec za tveganja

4.2.1 Je lastnik te politike in zagotavlja njeno usklajenost s standardoma ISO/IEC 27001 in ISO/IEC 27005.

4.2.2 Vodi organizacijski proces ocenjevanja tveganj ter vzdržuje register tveganj in načrt obravnave tveganj.

4.2.3 Zagotavlja periodične preglede in eskalacijo ključnih tveganj izvršnemu vodstvu ali usmerjevalnemu odboru ISMS.

[... 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 Ta politika in z njo povezani okvir se morata pregledati letno ali:

9.1.1 po večjem tveganem dogodku ali varnostnem incidentu,

9.1.2 po pomembni organizacijski ali tehnični spremembi,

9.1.3 kot odziv na ugotovitve presoje ali nove regulativne zahteve.

9.2 Vodja ISMS, pooblaščenec za tveganja in ekipa za skladnost so skupaj odgovorni za:

9.2.1 začetek cikla pregleda,

9.2.2 zbiranje prispevkov poslovnih enot,

9.2.3 revizijo postopkov in pragov po potrebi.

9.3 Vse spremembe morajo biti:

9.3.1 pod nadzorom različic in evidentirane,

9.3.2 odobrene s strani najvišjega vodstva,

9.3.3 sporočene zainteresiranim stranem,

9.3.4 hranjene v revizijskem repozitoriju najmanj 5 let.

10. Povezane politike in povezave

10.1 Ta politika je medsebojno odvisna od naslednjih politik informacijske varnosti:

10.1.1 P1 – Politika informacijske varnosti: določa celovit model upravljanja varnosti, v okviru katerega se izvaja ta politika obvladovanja tveganj.

10.1.2 P2 – Politika vlog in odgovornosti upravljanja: določa odgovorne lastnike in ravni upravljanja, na katere se sklicuje matrika eskalacije tveganj.

10.1.3 P5 – Politika upravljanja sprememb: sproži ponovno oceno tveganj pri spremembah infrastrukture in organizacije.

10.1.4 P13 – Politika klasifikacije in označevanja podatkov: podpira oceno vpliva med prepoznavanjem tveganj.

10.1.5 P33 – Politika spremljanja presoj in skladnosti: potrjuje skladnost s politiko, vključno s popolnostjo registra tveganj in dokazili o obravnavi.

11. Referenčni standardi in okviri

11.1 Ta politika je izrecno usklajena z naslednjimi standardi in okviri, da se zagotovi skladnost z mednarodnimi dobrimi praksami in regulativnimi pričakovanji na področju obvladovanja tveganj informacijske varnosti:

11.2 ISO/IEC 27001:

11.2.1 Klavzula 6.1: določa zahteve za prepoznavanje tveganj in priložnosti, vključno s celotnim življenjskim ciklom ocenjevanja in obravnave tveganj informacijske varnosti. Ta politika operativno izvaja klavzuli 6.1.2 in 6.1.3 prek strukturiranega okvira, ki zahteva dokumentirano prepoznavanje, analizo, vrednotenje in obravnavo tveganj ter protokole za sprejem preostalega tveganja.

11.2.2 Klavzula 8.32: vključitev razmišljanja na podlagi tveganj v procese upravljanja sprememb zagotavlja, da vse pomembne organizacijske spremembe sprožijo formalne ponovne ocene tveganj.

11.2.3 Klavzula 10: nenehno izboljševanje je vključeno prek rednih pregledov politike, analize trendov tveganj in posodobitev SoA, ki temeljijo na ugotovitvah o tveganjih.

11.3 ISO/IEC 27005:

11.3.1 Zagotavlja specializirane in podrobne smernice za obvladovanje tveganj informacijske varnosti. Ta politika izvaja celoten procesni model tveganj po ISO/IEC 27005: določitev konteksta, prepoznavanje tveganj, analiza tveganj, vrednotenje tveganj, obravnava tveganj, sprejem tveganja, komuniciranje tveganj ter spremljanje in pregled tveganj.

11.4 ISO 31000:

11.4.1 Ta politika vključuje načela ISO 31000, kot so zavezanost vodstva, vključitev v odločanje in nenehno izboljševanje. Zagotavlja, da je obvladovanje tveganj vključeno v kulturo in delovanje organizacije.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Usklajena je z navodili NIST za izvajanje ocen tveganj, vključno s prepoznavanjem groženj, analizo ranljivosti, oceno verjetnosti in določitvijo vpliva. Struktura te politike sledi korakom ocenjevanja tveganj, ki jih določa NIST, in jih prilagaja tehničnim ter poslovnim procesom.

11.6 NIST SP 800-39:

11.6.1 Podpira upravljanje tveganj na ravni podjetja s poudarkom na večnivojskem obvladovanju tveganj na ravni organizacije, poslanstva oziroma poslovnih procesov in informacijskih sistemov. Politika zagotavlja, da je lastništvo tveganj jasno določeno na vseh ravneh in vključuje strategije obravnave na ravni organizacije.

11.7 Uredba EU GDPR:

11.7.1 Člen 24: zahteva izvajanje ustreznih tehničnih in organizacijskih ukrepov za zagotovitev ustreznega obvladovanja tveganj varstva podatkov — to je obravnavano s strukturiranim procesom tveganj iz te politike.

11.7.2 Člen 25: »varstvo podatkov že pri načrtovanju in privzeto« je usklajeno z vključevanjem obravnave tveganj v zasnovo sistemov in procesov.

11.7.3 Člen 32: zahteva pristop k varnostnim ukrepom na podlagi tveganj — izpolnjeno z vrednotenjem tveganj na podlagi vpliva in izbiro kontrol na podlagi tveganj.

11.8 Direktiva EU NIS2:

11.8.1 Člen 21(2)(a–d): od subjektov zahteva izvajanje ocen tveganj, uvedbo politik analize tveganj in zagotavljanje sorazmernih varnostnih ukrepov. Ta politika izpolnjuje te obveznosti z nenehno uporabo življenjskega cikla tveganj in dokumentiranim upravljanjem.

11.9 Uredba EU DORA:

11.9.1 Člen 5: zahteva dokumentiran okvir za upravljanje IKT-tveganj — v celoti pokrito z arhitekturo te politike, vključno s preslikavo SoA in KRI.

11.9.2 Člen 6: zahteva vključitev obvladovanja tveganj v strategije operativne odpornosti, kar je obravnavano z matrikami eskalacije in spremljanjem kritičnih sredstev.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: neposredno ustreza vzpostavitvi strukturiranega pristopa organizacije k obvladovanju tveganj, dodeljevanju vlog, spremljanju obravnave in zagotavljanju odgovornosti na ravni upravnega odbora.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: odraža se v osredotočenosti te politike na analizo trendov, spremljanje KRI ter vključevanje revizijskih povratnih informacij v zanke nenehnega izboljševanja.