					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P32					Naslov dokumenta: **Politika neprekinjenega poslovanja in obnovitve po nesreči**							
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 8	
ISO/IEC 27002:2022	Kontroli 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 do CP-11	
NIST SP 800-34 Rev.1	Načrtovanje ukrepov ob nepredvidenih dogodkih	Okvir
ISO 22301:2019		Zahteve za sistem upravljanja neprekinjenega poslovanja
Uredba EU GDPR	Člen 32	
Direktiva EU NIS2	Člen 21(2)(f)	
Uredba EU DORA	Člen 10	
COBIT 2019	DSS	

1. Namen

1.1. Ta politika določa obvezne kontrole in odgovornosti za zagotavljanje zmožnosti organizacije, da med motilnim incidentom in po njem ohrani ali obnovi kritične poslovne dejavnosti ter podporne sisteme IKT.

1.2. Njen namen je varovati življenja, operativno stabilnost, pravne obveznosti, zaveze do strank in ugled organizacije z vgrajevanjem odpornosti prek proaktivnega načrtovanja in preverjenih zmogljivosti obnovitve.

1.3. Ta politika predstavlja temelj okvira organizacije za upravljanje neprekinjenega poslovanja (BCM) in obnovitev po nesreči (DR) ter zagotavlja skladnost z veljavnimi regulativnimi, pogodbenimi in panožnimi zahtevami.

2. Področje uporabe

2.1. Ta politika se uporablja za vse organizacijske enote, informacijske sisteme, poslovne procese, osebje in storitve tretjih oseb, ki so na podlagi analize vpliva na poslovanje (BIA) razvrščeni kot kritični ali bistveni.

2.2. Politika zajema:

2.2.1. naravne in človeško povzročene motnje, vključno s kibernetskimi napadi, odpovedmi infrastrukture, izpadi podatkovnih centrov, pandemijami in prekinitvami storitev dobaviteljev;

2.2.2. načrtovanje, testiranje in stalno izboljševanje načrtov neprekinjenega poslovanja (BCP) in načrtov obnovitve po nesreči (DRP);

2.2.3. vloge in odgovornosti za odzivanje v izrednih razmerah, koordinacijo obnovitve in eskalacijo incidentov.

2.3. Določbe te politike veljajo za vse zaposlene in druge osebe z odgovornostmi na področju neprekinjenega poslovanja ali obnovitve, vključno z IT, lastniki poslovnih procesov, kriznimi vodji in dobavitelji.

3. Cilji

3.1. Zagotoviti neprekinjeno izvajanje poslovanja in storitev z vnaprej določenimi in preizkušenimi postopki ter zmanjšati operativni vpliv, škodo za ugled in pravne posledice.

3.2. Obnoviti storitve IKT v okviru določenih ciljnih časov obnovitve (RTO) in ciljnih točk obnovitve (RPO), usklajenih s stopnjami tolerance poslovnega tveganja.

3.3. Določiti lastništvo načrtovanja, izvajanja in upravljanja neprekinjenega poslovanja ter obnovitve po nesreči v celotni organizaciji.

3.4. Zagotoviti, da se zmogljivosti neprekinjenega poslovanja redno testirajo, vzdržujejo in izboljšujejo na podlagi realističnih scenarijev in ugotovitev presoj.

3.5. Izpolnjevati obveznosti skladnosti po standardih ISO, NIST, GDPR, DORA in NIS2 ter podpirati dolžno skrbnost na področju operativne odpornosti in razpoložljivosti.

4. Vloge in odgovornosti

4.1. Najvišje vodstvo

4.1.1. odobri Politiko neprekinjenega poslovanja in obnovitve po nesreči ter zagotovi njeno strateško usklajenost;

4.1.2. dodeli proračun in vire za podporo neprekinjenemu poslovanju, odzivanju v izrednih razmerah in vajam obnovitve.

4.2. Vodja neprekinjenega poslovanja

4.2.1. je odgovoren za razvoj in vzdrževanje načrtov neprekinjenega poslovanja (BCP) na ravni celotne organizacije ter za koordinacijo testiranja neprekinjenega poslovanja;

4.2.2. vzdržuje načrt izvajanja analize vpliva na poslovanje (BIA), usklajuje usposabljanja in zagotavlja, da dokumentacija izpolnjuje zahteve skladnosti.

[... 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. To politiko morata vodja neprekinjenega poslovanja in vodja informacijske varnosti (CISO) pregledati letno, da se zagotovi usklajenost z:

9.1.1. spremembami poslovanja, kritičnih sistemov ali infrastrukture;

9.1.2. spoznanji iz incidentov, presoj, namiznih vaj ali testov DR;

9.1.3. posodobljenimi regulativnimi ali pogodbenimi obveznostmi (npr. DORA, GDPR, zahteve strank glede RTO/RPO);

9.1.4. spremembami apetita po tveganju ali strategije neprekinjenega poslovanja v organizaciji.

9.2. Pregledi morajo vključevati:

9.2.1. preverjanje ustreznosti načrtov in kontaktnih podatkov;

9.2.2. ponovno oceno RTO, RPO in razvrstitve ravni obnovitve;

9.2.3. oceno zmogljivosti storitev varnostnega kopiranja in DR;

9.2.4. povratne informacije deležnikov, ki so izvajali nedavne načrte obnovitve ali teste.

9.3. Vse spremembe politike morajo biti:

9.3.1. upravljane z različicami, z dokumentirano utemeljitvijo in potrditvijo deležnikov;

9.3.2. sporočene ključnemu osebju in ekipam s posodobljenimi odgovornostmi;

9.3.3. odražene v posodobljenih usposabljanjih, gradivih za ozaveščanje in operativnih postopkih.

9.4. Nujne vmesne posodobitve se morajo izdati, če pride do večje organizacijske spremembe, pravne zahteve ali kritične ugotovitve, zaradi katere obstoječi načrti ali politika niso več izvedljivi.

10. Povezane politike in povezave

10.1. Ta politika se izvaja usklajeno z naslednjimi ključnimi dokumenti:

10.1.1. P1 – Politika informacijske varnosti: določa zahtevo po delovanju na podlagi tveganj in odpornosti v vseh razmerah.

10.1.2. P5 – Politika upravljanja sprememb: zagotavlja, da vse spremembe konfiguracije ali infrastrukture, povezane z obnovitvijo, sledijo dokumentiranim in odobrenim postopkom.

10.1.3. P14 – Politika hrambe podatkov in odstranjevanja: ureja življenjski cikel medijev za varnostno kopiranje in obnovljenih podatkov, uporabljenih pri dejavnostih neprekinjenega poslovanja.

10.1.4. P15 – Politika varnostnega kopiranja in obnove: določa kontrole glede pogostosti varnostnega kopiranja, varnosti in preverjanja obnovitve.

10.1.5. P18 – Politika kriptografskih kontrol: zagotavlja, da postopki obnovitve ohranjajo standarde šifriranja in zaupnosti.

10.1.6. P22 – Politika beleženja in spremljanja: podpira zaznavanje in eskalacijo dogodkov, ki vplivajo na neprekinjeno poslovanje.

10.1.7. P30 – Politika odzivanja na incidente: določa procese zajezitve, eskalacije in analize temeljnega vzroka, usklajene s sprožilci neprekinjenega poslovanja.

10.1.8. P33 – Politika spremljanja presoje in skladnosti: preverja celovitost in učinkovitost praks neprekinjenega poslovanja in obnovitve v sistemih in procesih.

11. Referenčni standardi in okviri

11.1. Ta politika je usklajena z mednarodno priznanimi standardi za neprekinjeno poslovanje in obnovitev po nesreči ter podpira preverljivost, odpornost in pravno skladnost.

11.2. ISO/IEC 27002

11.2.1. Dodatek A, kontrola 5.29 – informacijska varnost med motnjami: zahteva neprekinjeno delovanje varnostnih kontrol v neugodnih razmerah.

11.2.2. Dodatek A, kontrola 5.30 – pripravljenost IKT za neprekinjeno poslovanje: zahteva pripravo, testiranje in potrjevanje zmogljivosti obnovitve IKT.

11.3. ISO 22301:2019 – sistemi upravljanja neprekinjenega poslovanja

11.3.1. Določa okvir za vzpostavitev, izvajanje in vzdrževanje praks BCM, usklajenih s cilji organizacije in pragovi tveganja.

11.4. NIST SP 800-34 Rev.1 – smernice za načrtovanje ukrepov ob nepredvidenih dogodkih

11.4.1. Opredeljuje dobre prakse za načrte ukrepanja ob nepredvidenih dogodkih za sisteme IT, vključno z razvojem strategije neprekinjenega poslovanja, analizo vpliva in testiranjem načrtov.

11.5. Uredba EU GDPR (2016/679)

11.5.1. Člen 32 – Varnost obdelave: zahteva odpornost sistemov obdelave ter pravočasno obnovitev razpoložljivosti in dostopa do osebnih podatkov po incidentu.

11.6. Direktiva EU NIS2 (2022/2555)

11.6.1. Člen 21(2)(f): zahteva ukrepe za neprekinjeno poslovanje in krizno upravljanje za podporo varnosti omrežnih in informacijskih sistemov.

11.7. Uredba EU DORA (2022/2554)

11.7.1. Člen 10 – neprekinjeno poslovanje IKT: zahteva, da finančni subjekti razvijejo in testirajo načrte neprekinjenega poslovanja IKT, vključno z RTO/RPO na podlagi tveganja in zmogljivostmi preklopa na rezervno okolje.

11.8. COBIT 2019

11.8.1. DSS04 – upravljanje neprekinjenega poslovanja: zajema vse vidike načrtovanja neprekinjenega poslovanja, vključno z identifikacijo groženj, analizo vpliva, strategijo obnovitve in rednim testiranjem.