					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P32S					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	Klavzule 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontrole 5.29, 5	
NIST SP 800-53 Rev. 5	CP-2, CP-4, CP-6, CP-7	
Uredba (EU) GDPR	Člena 32, 33	
Direktiva (EU) NIS2	Člen 21(2)(f)	
Uredba (EU) DORA	Člen 10	
COBIT 2019	DSS	

1. Namen

1.1 Ta politika zagotavlja, da organizacija med motilnimi dogodki in po njih ohrani poslovanje ter obnovi ključne IT-storitve v primeru izpadov električne energije, kibernetskih napadov, okužb z izsiljevalsko programsko opremo ali odpovedi sistemov.

1.2 Določa jasen okvir za načrtovanje neprekinjenega poslovanja in obnovitve po nesreči (BC/DR), prilagojen malim in srednjim podjetjem brez namenskih IT-ekip.

1.3 Ta politika organizaciji pomaga izpolnjevati obvezne zahteve po ISO/IEC 27001:2022, GDPR, NIS2, DORA in COBIT 2019 ter hkrati krepi operativno odpornost in zaupanje strank.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 vse poslovno kritične sisteme in storitve (npr. e-pošto, shranjevanje v oblaku, platforme za izdajanje računov, evidence o strankah),

2.1.2 vse zaposlene in zunanje ponudnike IT-storitev, odgovorne za pripravljenost in izvajanje BC/DR,

2.1.3 vse vrste motenj, vključno s kibernetskimi incidenti, odpovedmi strojne opreme, izpadi električne energije, poplavami in nedostopnostjo pisarn.

2.2 Zajema:

2.2.1 upravljanje varnostnega kopiranja,

2.2.2 načrtovanje neprekinjenega poslovanja (BCP),

2.2.3 aktivnosti obnovitve po nesreči,

2.2.4 usposabljanje zaposlenih in testiranje,

2.2.5 pravne in regulatorne postopke odzivanja.

3. Cilji

3.1 Zaščititi sposobnost organizacije za izvajanje ključnih storitev kljub nenačrtovanim motnjam.

3.2 Zagotoviti pravočasno obnovitev sistemov in podatkov z vnaprej določenimi ciljnimi časi obnovitve (RTO).

3.3 Zagotoviti, da vsi zaposleni v času kriz sledijo postopkom neprekinjenega poslovanja z minimalno mero nejasnosti.

3.4 Ohraniti skladnost z zakonodajo s področja varstva podatkov in operativne odpornosti, vključno s členom 32 GDPR in členom 21 Direktive (EU) NIS2.

3.5 Vzpostaviti praktično in preverljivo strategijo neprekinjenega poslovanja in obnovitve, primerno za mala in srednja podjetja.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 je lastnik procesa BC/DR in te politike,

4.1.2 odobri načrt neprekinjenega poslovanja (BCP),

4.1.3 usklajuje odziv na incidente in interno komunikacijo med motnjami,

4.1.4 izvede regulatorna obveščanja, kadar so zahtevana (npr. prijavo kršitev po GDPR).

4.2 Ponudnik IT-podpore / sistemski skrbnik

4.2.1 vzdržuje in testira varnostne kopije,

4.2.2 izvede postopke obnovitve po nesreči, ko so aktivirani,

4.2.3 dokumentira vse aktivnosti obnovitve in dogodke ponovne vzpostavitve sistemov,

4.2.4 kritične IT-incidente nemudoma prijavi GM.

[... 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 in načrta

9.1.1 Generalni direktor (GM) mora zagotoviti, da se ta politika in pripadajoči načrt neprekinjenega poslovanja (BCP) formalno pregledata najmanj enkrat letno.

9.1.2 Pregled mora vključevati:

9.1.2.1 oceno novih ali nastajajočih tveganj,

9.1.2.2 ponovno potrditev vrednosti RTO/RPO,

9.1.2.3 preverjanje informacij o dobaviteljih in kontaktih,

9.1.2.4 uskladitev s spremembami v IT-sistemih, pravnih obveznostih ali poslovanju.

9.2 Posodobitve na podlagi sprožilcev

9.2.1 Ta politika mora biti posodobljena tudi kot odziv na:

9.2.1.1 večje incidente ali motnje, zlasti če cilji niso bili doseženi,

9.2.1.2 nove pravne ali regulatorne obveznosti (npr. spremembe DORA),

9.2.1.3 spremembe kritičnih sistemov, platform v oblaku ali osebja,

9.2.1.4 ugotovitve iz letnih testov BCP/DR.

9.3 Postopek nadzora sprememb

9.3.1 Vse spremembe mora odobriti GM.

9.3.2 Voditi je treba evidenco različic, ki vključuje datum, opis spremembe in odobritelja.

9.3.3 Posodobljena politika mora biti ponovno posredovana vsem relevantnim osebam, vključno s ponudnikom IT-podpore in vodji oddelkov.

9.4 Dokumentiranje pridobljenih spoznanj

9.4.1 Dokumentirana spoznanja po testih ali dejanskih motnjah morajo biti vključena v prihodnje revizije.

9.4.2 Ti pregledi morajo vključevati tudi ocene uspešnosti dobaviteljev in preverjanje ustreznosti odziva.

10. Povezane politike in povezave

10.1 Ta politika je tesno povezana z naslednjimi politikami za SME:

10.1.1 P1S – P01 Politika informacijske varnosti: določa krovne varnostne cilje, ki jih morajo podpirati prakse neprekinjenega poslovanja in obnovitve.

10.1.2 P4S – Politika nadzora dostopa: omogoča nujni preklic ali ponovno vzpostavitev uporabniškega dostopa v scenarijih poslovnih motenj.

10.1.3 P6S – Politika upravljanja tveganj: predstavlja temelj za identifikacijo, vrednotenje in določanje prioritet tveganj, povezanih z neprekinjenim poslovanjem.

10.1.4 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da so zaposleni pripravljeni ukrepati med motnjami in razumejo BCP.

10.1.5 P15S – Politika varnostnega kopiranja in obnove: določa posebne tehnične postopke za zagotavljanje razpoložljivosti podatkov in obnovitve.

10.1.6 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da načrtovanje neprekinjenega poslovanja spoštuje varstvo osebnih podatkov ter da je med incidenti in po njih skladno z GDPR.

10.1.7 P22S – Politika beleženja in spremljanja: podpira zaznavanje dogodkov, ki lahko sprožijo procese BC/DR, ter zagotavlja forenzične revizijske sledi po motnji.

10.1.8 P30S – Politika odzivanja na incidente: neposredno predhodi aktivaciji procesa obnovitve ob kibernetskih ali operativnih incidentih.

10.1.9 P31S – Politika zbiranja dokazov in forenzične preiskave: zagotavlja, da se med scenariji neprekinjenega poslovanja zajamejo digitalni dokazi za potrebe skladnosti, zavarovanja ali preiskave.

10.2 Te politike skupaj tvorijo skladen okvir, pripravljen za presojo, za odpornost, odgovornost in neprekinjeno delovanje kontrol v vseh dejavnostih SME.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:

11.1.1 Klavzula 6.1 – zahteva načrtovanje in obravnavo na podlagi tveganj, vključno z neprekinjenim poslovanjem in obnovitvijo.

11.1.2 Klavzula 6.3 – poudarja nenehno izboljševanje po motnjah.

11.1.3 Klavzula 8.1 – zahteva operativne kontrole, ki vključujejo dokumentirane ukrepe neprekinjenega poslovanja.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 5.29 – zahteva vzpostavitev in vzdrževanje ureditev za neprekinjeno poslovanje.

11.2.2 Kontrola 5.30 – zahteva testiranje in pregled teh ureditev.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 CP-2 – opredeljuje zahteve za načrtovanje ukrepov ob nepredvidenih dogodkih.

11.3.2 CP-4 – zahteva usposabljanje osebja organizacije za ukrepanje ob nepredvidenih dogodkih.

11.3.3 CP-6 – zajema zahteve glede alternativne lokacije za hrambo.

11.3.4 CP-7 – določa zahteve glede alternativne lokacije za obdelavo.

11.4 Uredba (EU) GDPR:

11.4.1 Člen 32 – zahteva ukrepe za zagotavljanje stalne razpoložljivosti in odpornosti sistemov in storitev obdelave.

11.4.2 Člen 33 – sproži obveznosti obveščanja o kršitvah v primerih, ko odpoved neprekinjenega poslovanja povzroči kompromitacijo osebnih podatkov.

11.5 Direktiva (EU) NIS2 (2022/2555):

11.5.1 Člen 21(2)(f) – zahteva zmogljivosti za načrtovanje neprekinjenega poslovanja in krizno upravljanje kot pogoj pripravljenosti na kibernetska tveganja.

11.6 Uredba (EU) DORA (2022/2554):

11.6.1 Člen 10 – zahteva uvedbo testiranja digitalne operativne odpornosti in zmogljivosti obnovitve, zlasti za mala in srednja podjetja v finančnem sektorju.

11.7 COBIT 2019:

11.7.1 DSS04 – Upravljanje neprekinjenega poslovanja: zagotavlja usmeritve za korporativno upravljanje za ohranjanje in potrjevanje operativne odpornosti, vključno z lastništvom, testiranjem, vključevanjem dobaviteljev in pregledi po dogodkih.