					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P32S					Naziv dokumenta: **Politika neprekidnosti poslovanja i oporavka od katastrofe**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1, 6.3, 8	
ISO/IEC 27002:2022	Kontrole 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR EU	Članci 32, 33	
Direktiva EU NIS2	Članak 21(2)(f)	
Uredba EU DORA	Članak 10	
COBIT 2019	DSS04	

1. Svrha

1.1 Ova politika osigurava da organizacija može održavati poslovne aktivnosti i oporaviti ključne IT usluge tijekom i nakon poremećaja, kao što su prekidi napajanja, kibernetički napadi, napadi ucjenjivačkim softverom ili kvarovi sustava.

1.2 Ovom se politikom uspostavlja jasan okvir za planiranje neprekidnosti poslovanja i oporavka od katastrofe (BC/DR), prilagođen malim i srednjim poduzećima bez namjenskih IT timova.

1.3 Ova politika pomaže organizaciji ispuniti obvezne zahtjeve iz standarda ISO/IEC 27001:2022, GDPR-a, Direktive EU NIS2, Uredbe EU DORA i COBIT-a 2019, uz istodobno jačanje operativne otpornosti i povjerenja korisnika.

2. Područje primjene

2.1 Ova se politika primjenjuje na:

2.1.1 sve poslovno kritične sustave i usluge (npr. e-poštu, pohranu u oblaku, platforme za izdavanje računa, evidencije o klijentima)

2.1.2 sve zaposlenike i vanjske pružatelje IT usluga odgovorne za spremnost i provedbu BC/DR-a

2.1.3 sve vrste poremećaja, uključujući kibernetičke incidente, kvarove hardvera, gubitak napajanja, poplave i nedostupnost uredskog prostora

2.2 Ova politika obuhvaća:

2.2.1 upravljanje sigurnosnim kopijama

2.2.2 planiranje neprekidnosti poslovanja (BCP)

2.2.3 postupke oporavka od katastrofe

2.2.4 osposobljavanje zaposlenika i testiranje

2.2.5 pravne i regulatorne postupke odgovora

3. Ciljevi

3.1 Zaštititi sposobnost organizacije da pruža ključne usluge unatoč neplaniranim poremećajima.

3.2 Osigurati pravodoban oporavak sustava i podataka uz unaprijed definirane ciljeve vremena oporavka (RTO).

3.3 Omogućiti svim zaposlenicima da tijekom kriznih situacija slijede postupke neprekidnosti uz minimalan rizik od zabune.

3.4 Održavati usklađenost sa zakonima o zaštiti podataka i operativnoj otpornosti, uključujući članak 32. GDPR-a i članak 21. Direktive EU NIS2.

3.5 Uspostaviti praktičnu i provjerljivu strategiju neprekidnosti i oporavka primjerenu malim i srednjim poduzećima.

4. Uloge i odgovornosti

4.1 Generalni direktor (GM)

4.1.1 odgovoran je za BC/DR proces i ovu politiku

4.1.2 odobrava Plan neprekidnosti poslovanja (BCP)

4.1.3 koordinira odgovor na incidente i internu komunikaciju tijekom poremećaja

4.1.4 prema potrebi provodi regulatorne prijave i obavijesti (npr. prijavu povrede osobnih podataka prema GDPR-u)

4.2 Pružatelj IT usluga / administrator sustava

4.2.1 održava i testira sigurnosne kopije

4.2.2 provodi postupke oporavka od katastrofe kada se aktiviraju

4.2.3 dokumentira sve aktivnosti oporavka i događaje ponovne uspostave rada sustava

4.2.4 bez odgode prijavljuje GM-u kritične IT incidente

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled politike i plana

9.1.1 Generalni direktor (GM) mora osigurati da se ova politika i pripadajući Plan neprekidnosti poslovanja (BCP) formalno pregledaju najmanje jednom godišnje.

9.1.2 Pregled mora uključivati:

9.1.2.1 procjenu novih ili nastajućih rizika

9.1.2.2 ponovnu provjeru RTO-a/RPO-a

9.1.2.3 provjeru podataka o dobavljačima i kontaktima

9.1.2.4 usklađivanje s promjenama u IT sustavima, pravnim obvezama ili poslovanju

9.2 Ažuriranja na temelju okidača

9.2.1 Ova se politika mora ažurirati i kao odgovor na:

9.2.1.1 velike incidente ili poremećaje, osobito ako ciljevi nisu ostvareni

9.2.1.2 nove pravne ili regulatorne obveze (npr. izmjene Uredbe EU DORA)

9.2.1.3 promjene u ključnim sustavima, platformama u oblaku ili osoblju

9.2.1.4 nalaze iz godišnjih BCP/DR testova

9.3 Postupak upravljanja promjenama

9.3.1 Sve promjene mora odobriti GM.

9.3.2 Mora se voditi evidencija povijesti verzija, uključujući datum, opis promjene i odobritelja.

9.3.3 Ažurirana politika mora se ponovno distribuirati svom relevantnom osoblju, uključujući pružatelja IT usluga i voditelje odjela.

9.4 Dokumentiranje utvrđenih pouka

9.4.1 Nakon testova ili stvarnih poremećaja, dokumentirane utvrđene pouke moraju se uključiti u buduća ažuriranja.

9.4.2 Ti pregledi moraju uključivati i ocjene uspješnosti dobavljača te provjere primjerenosti odgovora.

10. Povezane politike i poveznice

10.1 Ova je politika usko povezana sa sljedećim politikama za mala i srednja poduzeća:

10.1.1 P1S – Politika informacijske sigurnosti: definira sigurnosne ciljeve visoke razine koje prakse neprekidnosti i oporavka moraju podupirati.

10.1.2 P4S – Politika kontrole pristupa: omogućuje hitno opozivanje ili ponovnu uspostavu korisničkog pristupa u scenarijima poslovnih poremećaja.

10.1.3 P6S – Politika upravljanja rizicima: čini temelj za identifikaciju, procjenu i određivanje prioriteta rizika povezanih s neprekidnošću poslovanja.

10.1.4 P8S – Politika podizanja svijesti o informacijskoj sigurnosti i osposobljavanja: osigurava da su zaposlenici spremni postupati tijekom poremećaja i da razumiju BCP.

10.1.5 P15S – Politika sigurnosnog kopiranja i vraćanja podataka: propisuje specifične tehničke postupke za očuvanje dostupnosti podataka i oporavak.

10.1.6 P17S – Politika zaštite podataka i privatnosti: osigurava da planiranje neprekidnosti poslovanja poštuje zaštitu osobnih podataka i usklađenost s GDPR-om tijekom i nakon incidenata.

10.1.7 P22S – Politika zapisivanja događaja i praćenja: podržava otkrivanje događaja koji mogu pokrenuti BC/DR procese i osigurava revizijske tragove za forenzičke potrebe nakon poremećaja.

10.1.8 P30S – Politika odgovora na incidente: neposredno prethodi aktivaciji procesa oporavka u slučaju kibernetičkih ili operativnih incidenata.

10.1.9 P31S – Politika prikupljanja dokaza i digitalne forenzike: osigurava prikupljanje digitalnih dokaza tijekom scenarija neprekidnosti poslovanja za potrebe usklađenosti, osiguranja ili istrage.

10.2 Ove politike čine povezani okvir za otpornost, odgovornost i kontinuitet kontrola u svim poslovnim aktivnostima malih i srednjih poduzeća, spreman za reviziju.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:

11.1.1 Točka 6.1 – zahtijeva planiranje i obradu rizika na temelju procjene rizika, uključujući neprekidnost poslovanja i oporavak.

11.1.2 Točka 6.3 – naglašava kontinuirano poboljšavanje nakon poremećaja.

11.1.3 Točka 8.1 – propisuje operativne kontrole, uključujući dokumentirane mjere neprekidnosti poslovanja.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 5.29 – zahtijeva uspostavu i održavanje aranžmana za neprekidnost poslovanja.

11.2.2 Kontrola 5.30 – zahtijeva testiranje i preispitivanje tih aranžmana.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – definira zahtjeve za planiranje nepredviđenih okolnosti.

11.3.2 CP-4 – propisuje osposobljavanje osoblja organizacije za postupanje u nepredviđenim okolnostima.

11.3.3 CP-6 – obuhvaća zahtjeve za alternativnu lokaciju za pohranu.

11.3.4 CP-7 – uređuje očekivanja za alternativnu lokaciju za obradu.

11.4 GDPR EU:

11.4.1 Članak 32 – zahtijeva mjere za osiguranje trajne dostupnosti i otpornosti sustava obrade i usluga.

11.4.2 Članak 33 – aktivira obveze prijave povrede u slučajevima kada poremećaj neprekidnosti dovede do ugrožavanja osobnih podataka.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članak 21(2)(f) – zahtijeva planiranje neprekidnosti poslovanja i sposobnosti upravljanja krizama kao uvjet spremnosti na kibernetičke rizike.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Članak 10 – propisuje provedbu testiranja digitalne operativne otpornosti i sposobnosti oporavka, osobito za mala i srednja poduzeća u financijskom sektoru.

11.7 COBIT 2019:

11.7.1 DSS04 – Upravljanje neprekidnošću: pruža smjernice za korporativno upravljanje radi održavanja i provjere operativne otpornosti, uključujući vlasništvo, testiranje, uključivanje dobavljača i preglede nakon događaja.