					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P32					Naziv dokumenta: **Politika kontinuiteta 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/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	
ISO/IEC 27002:2022	Kontrole 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 do CP-11	
NIST SP 800-34 Rev.1	Planiranje kontinuiteta	Okvir
ISO 22301:2019		Zahtjevi za sustav upravljanja kontinuitetom poslovanja
GDPR EU	Članak 32	
Direktiva EU NIS2	Članak 21(2)(f)	
Uredba EU DORA	Članak 10	
COBIT 2019	DSS	

1. Svrha

1.1. Ova politika utvrđuje obvezne kontrole i odgovornosti za osiguravanje sposobnosti organizacije da održi ili obnovi kritične poslovne operacije i pripadajuće IKT usluge tijekom i nakon incidenta koji uzrokuje prekid poslovanja.

1.2. Svrha ove politike jest zaštita života, operativne stabilnosti, zakonskih obveza, obveza prema korisnicima i ugleda organizacije uspostavom otpornosti kroz proaktivno planiranje i provjerene sposobnosti oporavka.

1.3. Ova politika čini osnovu okvira za upravljanje kontinuitetom poslovanja (BCM) i oporavak od katastrofe (DR) te osigurava usklađenost s primjenjivim regulatornim, ugovornim i sektorskim zahtjevima.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve organizacijske jedinice, informacijske sustave, poslovne procese, osoblje i usluge trećih strana koji su, na temelju rezultata analize utjecaja na poslovanje (BIA), klasificirani kao kritični ili ključni.

2.2. Politika obuhvaća:

2.2.1. prirodne i ljudskim djelovanjem uzrokovane prekide, uključujući kibernetičke napade, kvarove infrastrukture, prekide rada podatkovnih centara, pandemije i prekide usluga dobavljača

2.2.2. planiranje, testiranje i kontinuirano unaprjeđenje planova kontinuiteta poslovanja (BCP) i planova oporavka od katastrofe (DRP)

2.2.3. uloge i odgovornosti za odgovor na izvanredne događaje, koordinaciju oporavka i eskalaciju incidenata

2.3. Sve osobe s odgovornostima u području kontinuiteta poslovanja ili oporavka, uključujući IT, vlasnike poslovnih procesa, voditelje kriznog upravljanja i dobavljače, obvezne su postupati u skladu s ovom politikom.

3. Ciljevi

3.1. Osigurati kontinuitet poslovnih operacija i usluga putem unaprijed definiranih i testiranih postupaka te svesti na najmanju moguću mjeru operativni, reputacijski i pravni učinak.

3.2. Oporaviti IKT usluge unutar definiranih ciljnih vremena oporavka (RTO) i ciljnih točaka oporavka (RPO), usklađenih s razinama tolerancije na poslovni rizik.

3.3. Dodijeliti vlasništvo nad planiranjem, provedbom i upravljanjem kontinuitetom poslovanja i oporavkom od katastrofe na razini cijele organizacije.

3.4. Osigurati da se sposobnosti kontinuiteta redovito testiraju, održavaju i unaprjeđuju na temelju realističnih scenarija i revizijskih nalaza.

3.5. Ispuniti obveze usklađenosti prema ISO, NIST-u, GDPR-u, DORA-i i NIS2, uz dokazivanje dužne pažnje u području operativne otpornosti i raspoloživosti.

4. Uloge i odgovornosti

4.1. Izvršno rukovodstvo

4.1.1. Odobrava Politiku kontinuiteta poslovanja i oporavka od katastrofe te osigurava njezinu stratešku usklađenost.

4.1.2. Dodjeljuje proračun i resurse za podršku kontinuitetu poslovanja, odgovoru na izvanredne događaje i vježbama oporavka.

4.2. Voditelj kontinuiteta poslovanja (BCM Lead)

4.2.1. Odgovoran je za izradu i održavanje BCP-ova na razini cijele organizacije te za koordinaciju testiranja kontinuiteta poslovanja.

4.2.2. Održava raspored provedbe BIA-e, organizira osposobljavanje i osigurava da dokumentacija ispunjava zahtjeve usklađenosti.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Ovu politiku moraju najmanje jednom godišnje pregledati voditelj kontinuiteta poslovanja i CISO kako bi se osigurala usklađenost sa sljedećim:

9.1.1. promjenama u poslovnim operacijama, kritičnim sustavima ili infrastrukturi

9.1.2. naučenim lekcijama iz incidenata, revizija, stolnih vježbi ili DR testiranja

9.1.3. ažuriranim regulatornim ili ugovornim obvezama (npr. DORA, GDPR, zahtjevi korisnika za RTO/RPO)

9.1.4. promjenama u organizacijskoj sklonosti riziku ili strategiji kontinuiteta poslovanja

9.2. Pregledi moraju uključivati:

9.2.1. provjeru relevantnosti planova i podataka za kontakt

9.2.2. ponovno vrednovanje RTO-a, RPO-a i razvrstavanja po razinama oporavka

9.2.3. procjenu kapaciteta usluga sigurnosnog kopiranja i DR-a

9.2.4. povratne informacije dionika koji su provodili nedavne planove oporavka ili testiranja

9.3. Sve promjene politike moraju biti:

9.3.1. pod nadzorom verzija, s dokumentiranim obrazloženjem i potvrdom relevantnih dionika

9.3.2. priopćene ključnom osoblju i timovima s ažuriranim odgovornostima

9.3.3. odražene u ažuriranim materijalima za osposobljavanje, podizanje svijesti i operativnim postupcima

9.4. Hitna privremena ažuriranja moraju se izdati ako dođe do velike organizacijske promjene, zakonskog naloga ili kritičnog nalaza zbog kojeg postojeći planovi ili ova politika više nisu provedivi.

10. Povezane politike i poveznice

10.1. Ova politika primjenjuje se u koordinaciji sa sljedećim ključnim dokumentima:

10.1.1. P1 – Politika informacijske sigurnosti: utvrđuje zahtjev za otpornim operacijama utemeljenima na riziku u svim uvjetima.

10.1.2. P5 – Politika upravljanja promjenama: osigurava da sve promjene konfiguracije ili infrastrukture povezane s oporavkom slijede dokumentirane i odobrene tijekove rada.

10.1.3. P14 – Politika zadržavanja i zbrinjavanja podataka: uređuje životni ciklus medija za sigurnosne kopije i oporavljenih podataka koji se koriste u aktivnostima kontinuiteta poslovanja.

10.1.4. P15 – Politika izrade sigurnosnih kopija i obnove: propisuje kontrole učestalosti izrade sigurnosnih kopija, njihove sigurnosti i provjere obnove.

10.1.5. P18 – Politika kriptografskih kontrola: osigurava da procesi oporavka poštuju standarde šifriranja i povjerljivosti.

10.1.6. P22 – Politika zapisivanja i praćenja: podržava otkrivanje i eskalaciju događaja koji utječu na kontinuitet poslovanja.

10.1.7. P30 – Politika odgovora na incidente: definira procese obuzdavanja, eskalacije i utvrđivanja temeljnog uzroka usklađene s okidačima kontinuiteta poslovanja.

10.1.8. P33 – Politika revizije i praćenja usklađenosti: provjerava cjelovitost i učinkovitost praksi kontinuiteta poslovanja i oporavka kroz sustave i procese.

11. Referentni standardi i okviri

11.1. Ova politika usklađena je s međunarodno prihvaćenim standardima kontinuiteta poslovanja i oporavka od katastrofe te podupire mogućnost revizije, otpornost i pravnu usklađenost.

11.2. ISO/IEC 27002

11.2.1. Dodatak A, kontrola 5.29 – Informacijska sigurnost tijekom prekida: zahtijeva kontinuitet sigurnosnih kontrola u nepovoljnim uvjetima.

11.2.2. Dodatak A, kontrola 5.30 – Spremnost IKT-a za kontinuitet poslovanja: nalaže pripremu, testiranje i potvrdu sposobnosti oporavka IKT-a.

11.3. ISO 22301:2019 – Sustavi upravljanja kontinuitetom poslovanja

11.3.1. Pruža okvir za uspostavu, provedbu i održavanje praksi BCM-a usklađenih s organizacijskim ciljevima i pragovima rizika.

11.4. NIST SP 800-34 Rev.1 – Vodič za planiranje kontinuiteta

11.4.1. Opisuje najbolju praksu za planove kontinuiteta IT sustava, uključujući razvoj strategije kontinuiteta, analizu učinka i testiranje planova.

11.5. GDPR EU (2016/679)

11.5.1. Članak 32 – Sigurnost obrade: zahtijeva otpornost sustava obrade te pravodobnu obnovu dostupnosti i pristupa osobnim podacima nakon incidenta.

11.6. Direktiva EU NIS2 (2022/2555)

11.6.1. Članak 21(2)(f): nalaže mjere kontinuiteta poslovanja i kriznog upravljanja radi potpore sigurnosti mrežnih i informacijskih sustava.

11.7. Uredba EU DORA (2022/2554)

11.7.1. Članak 10 – IKT kontinuitet poslovanja: zahtijeva da financijski subjekti izrade i testiraju planove kontinuiteta IKT-a, uključujući RTO/RPO utemeljene na riziku i mogućnosti prebacivanja na pričuvnu lokaciju.

11.8. COBIT 2019

11.8.1. DSS04 – Upravljanje kontinuitetom: obuhvaća sve aspekte planiranja kontinuiteta poslovanja, uključujući identifikaciju prijetnji, analizu učinka, strategiju oporavka i redovito testiranje.