



POLITIKA NEPREKINJENEGA POSLOVANJA – vzorčna dokumentacija

Različica:	1.0
Datum veljavnosti:	
Avtor:	
Odobril:	

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Politika neprekinjenega poslovanja« iz 4. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1). Dokument je generičen in je namenjen kot pomoč pri doseganju skladnosti predvsem malim in srednje velikim organizacijam v Republiki Sloveniji (do približno 200 uporabnikov oziroma naprav), ki morajo izpolnjevati zahteve iz ZInfV-1¹.

Politika neprekinjenega poslovanja je osrednji dokument, ki določa zavezo organizacije, da bo tudi ob resnih motnjah, izrednih dogodkih ali krizah zagotavljala kontinuirano izvajanje svojih ključnih storitev oziroma funkcij. Dokument predstavlja obvezujoč okvir za vzpostavitev, vzdrževanje in nenehno izboljševanje sistema upravljanja neprekinjenega poslovanja (SUNP) v skladu z ZInfV-1.

Dokument je vzorčen in generičen, zato ga mora organizacija prilagoditi svojim specifičnim potrebam: trenutnemu stanju informacijsko-komunikacijske infrastrukture, posebnostim sektorja (npr. zdravstveni, energetski, javna uprava), obsegu poslovanja, značilnim grožnjam po pristopu »upoštevanja vseh nevarnosti« (ang. *all-hazards approach*) ter veljavnim sektorskim predpisom. Dokument podpiše oziroma potrdi vodstvo organizacije, pregleda pa ga najmanj enkrat letno.

Dokument predstavlja poenostavljeno politiko neprekinjenega poslovanja, zasnovano tako, da je dovolj jasna in razumljiva za vodstvo in zaposlene, obenem pa dovolj strukturirana, da omogoča doseganje pričakovanih rezultatov pri zagotavljanju neprekinjenega poslovanja. Kljub poenostavljeni obliki politika zagotavlja vse bistvene elemente, ki jih zahtevata tako ZInfV-1 kot standard ISO/IEC 22301, in omogoča učinkovito doseganje pričakovanih rezultatov – to je zmanjšanje časa izpada ključnih procesov, zaščito ugleda in ohranjanje zaupanja deležnikov.

Uporabljeni viri:

- *Zakon o informacijski varnosti (Uradni list RS, št. 40/25);*
- *Izvedbena uredba Komisije (EU) 2024/2690, z dne 17. oktobra 2024, o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih trgov, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *Standard ISO/IEC 22301:2019;*
- *Technical Implementation Guidance on Cybersecurity Risk Management Measures, ENISA, junij 2025.*²

¹ Zavezanci iz ZInfV-1, ki so ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnega centra, ponudniki omrežij za dostavo vsebin, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev, ponudniki spletnih trgov, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudniki storitev zaupanja, morajo pri pripravi tega dokumenta upoštevati določbe Izvedbene uredbe Komisije (EU) št. 2024/2690, z dne 17. oktobra 2024.

² (https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf)



KAZALO

1.	Namen dokumenta	4
2.	Obseg	4
3.	Cilji in načela zagotavljanja neprekinjenega poslovanja.....	4
4.	Sistem upravljanja neprekinjenega poslovanja.....	5
5.	Določitev vlog in odgovornosti	5
6.	Popis poslovnih funkcij oziroma poslovnih procesov.....	6
7.	Analiza vplivov na poslovanje (ang. BIA – Business Impact Analysis).....	6
8.	Načrt neprekinjenega poslovanja (ang. BCP – Business Continuity Plan).....	7
8.1	Vsebina načrta:	7
8.2	Aktivacija načrta:	7
9.	Minimalna raven poslovanja	7
10.	Upravljanje varnostnih kopij in redundantnih zmogljivosti	8
11.	Vzdrževanje in izboljševanje.....	8



1. Namen dokumenta

Neprekinjeno poslovanje je ključna prednost in odgovornost [IME ORGANIZACIJE]. Vsi zaposleni so dolžni sodelovati pri izvajanju in spoštovanju te politike ter prispevati k večji odpornosti organizacije. Politika neprekinjenega poslovanja določa okvir za vzpostavitev, vzdrževanje in neprestano izboljševanje sistema upravljanja neprekinjenega poslovanja v skladu z zahtevami veljavnega Zakona o informacijski varnosti in po priporočilih standarda ISO 22301.

Namen te politike je opredelitev sistematičnega pristopa k zagotavljanju neprekinjenega poslovanja [IME ORGANIZACIJE] v primeru motenj, izrednih dogodkov ali kriznih situacij, da se lahko zagotavlja izvajanje ključnih storitev in nadaljuje s ključnimi poslovnimi funkcijami v tudi v primeru nepredvidenih dogodkov ali hujših motenj poslovanja.

Storitve oziroma poslovne funkcije so tiste, ki jih je [IME ORGANIZACIJE] po zakonu dolžna opravljati oziroma gre za dejavnost iz prilog Zakona o informacijski varnosti.

2. Obseg

Ta politika se nanaša na vse storitve, človeške vire, poslovne procese, prostore in opremo, informacije in informacijske sisteme (strojno in programsko opremo) ter storitve pogodbenih (zunanjih) izvajalcev [IME ORGANIZACIJE], potrebnih za zagotavljanje ključnih storitev oziroma funkcij, ki jih zagotavlja [IME ORGANIZACIJE].

Politika velja za vse poslovne enote, zaposlene in funkcije [IME ORGANIZACIJE] ter se nanaša na vse dejavnosti, ki so ključne za nadaljevanje delovanja in zagotavljanje ključnih storitev v primeru motenj.

3. Cilji in načela zagotavljanja neprekinjenega poslovanja

[IME ORGANIZACIJE] se zavezuje k:

- prepoznavanju ključnih poslovnih funkcij oziroma ključnih procesov in prepoznavanju tveganj, ki lahko vplivajo na njihovo delovanje;
- pripravi analize vplivov na poslovanje in načrta neprekinjenega poslovanja;
- zagotavljanju zadostnih virov za pripravo in izvajanje načrta neprekinjenega poslovanja;
- rednemu testiranju, posodabljanju in izboljševanju načrta neprekinjenega poslovanja;
- zagotavljanju minimalne ravni poslovanja v času motenj, kriz ali izrednih razmer;
- usposabljanju zaposlenih za delovanje v kriznih razmerah;
- spoštovanju zakonskih, regulatornih in pogodbenih obveznosti in
- sistematičnemu spremljanju in obravnavi ponavljajočih se incidentov ter neprestanemu izboljševanju sistema neprekinjenega poslovanja.

4. Sistem upravljanja neprekinjenega poslovanja

Sistem upravljanja neprekinjenega poslovanja [IME ORGANIZACIJE] omogoča, da tudi ob nepredvidenih dogodkih ali motnjah nadaljuje z izvajanjem ključnih poslovnih funkcij oziroma storitev. Njegovi cilji so zagotavljanje poslovne kontinuitete, varovanje virov in sredstev, izpolnjevanje zakonskih zahtev ter zaščita interesov deležnikov. Gre za strukturiran pristop, ki [IME ORGANIZACIJE] omogoča načrtovanje, izvajanje, spremljanje ter stalno izboljševanje postopkov in načrtov za ohranjanje neprekinjenega poslovanja. Sistem upravljanja neprekinjenega poslovanja obsega:

- to politiko neprekinjenega poslovanja;
- načrt neprekinjenega poslovanja;
- analizo vpliva na poslovanje in ocenjevanje tveganj, ki lahko vplivajo na neprekinjeno poslovanje;
- potrebne ukrepe in postopke za zagotovitev neprekinjenega poslovanja;
- preverjanje in testiranje načrtov neprekinjenega poslovanja v rednih časovnih obdobjih;
- zagotovila, da so vse zainteresirane strani seznanjene s postopki in načrti ter usposobljene za njihovo izvajanje in
- stalno izboljševanje sistema neprekinjenega poslovanja na podlagi rezultatov testiranj in izkušenj iz obravnavanih incidentov.

5

5. Določitev vlog in odgovornosti

Funkcija	Odgovornosti
Direktor / predstojnik organizacije	Zagotavlja strateške usmeritve, potrdi politiko in načrt; dodeli vire; zagotovi skladnost z zakonodajo, spremlja izvajanje politike.
Vodja neprekinjenega poslovanja	Skrbi za razvoj, posodabljanje in izvajanje politike, načrta neprekinjenega poslovanja in splošnega dela analize vplivov na poslovanje; koordinira krizno ekipo; organizira testiranja načrta.
IT oddelek / pogodbeni izvajalec	Upravljanje varnostnih kopij, zagotavljanje IT podpore in obnovitev sistemov; zagotavljanje redundantnih virov. Zagotavljanje ažurne in relevantne dokumentacije za nemoteno izvajanje navedenih aktivnosti.
Vsi zaposleni	Sodelujejo v usposabljanjih; poznajo in upoštevajo postopke neprekinjenega poslovanja, ki so relevantni za njihovo delo; poročajo o incidentih.
Krizna ekipa ³	Aktivira načrt; vodi odziv; komunicira z deležniki, vodstvom organizacije in pristojnimi organi; sodeluje pri testiranju načrtov.

Pri sodelovanju z zunanjimi (pogodbenimi) izvajalci je nujno zagotoviti, da se zanesljivost in sposobnost [IME ORGANIZACIJE] za izvajanje storitev ne zmanjšata. To vključuje

³ V manjših organizacijah so lahko naloge krizne ekipe prenesene na npr. vodjo neprekinjenega sodelovanja.

skrbno izbiro pogodbenih partnerjev, jasno opredeljene odgovornosti ter ustrezne nadzorne mehanizme, s katerimi se ohranja neprekinjeno in varno izvajanje storitev.

6. Popis poslovnih funkcij oziroma poslovnih procesov

Popis poslovnih funkcij oziroma poslovnih procesov se izvede za vse poslovne procese oziroma poslovne funkcije v [IME ORGANIZACIJE].

Vsakemu poslovnemu procesu se določi lastništvo in enoznačna oznaka procesa. Rezultat popisa poslovnih procesov je seznam poslovnih procesov, ki se preverja in po potrebi ažurira najmanj enkrat letno ali ob pomembnih spremembah.

Po izvedeni oceni vpliva na poslovanje za posamezne poslovne procese, se v seznamu poslovnih procesov ustrezno označijo poslovni procesi kot kritični, pomembni in podporni procesi.

Vsakemu procesu se v seznamu določi ali sodi v obseg minimalne ravni poslovanja.

Seznam poslovnih procesov (z navedbo potrebnih elementov) je v Prilogi I, ki je sestavni del te politike.

7. Analiza vplivov na poslovanje (ang. *Business Impact Analysis - BIA*)

6

Analiza vplivov na poslovanje se izvede za vse poslovne funkcije oziroma procese iz seznama poslovnih procesov. Analiza vplivov na poslovanje se izvaja oziroma preverja v rednih časovnih intervalih, najmanj pa enkrat letno, ob pomembnih spremembah ali pomembnih incidentih in vključuje najmanj:

- navedbo poslovnih funkcij oziroma procesov;
- navedbo lastnikov poslovnih procesov;
- oceno posledic prekinitve poslovanja (časovne, finančne, pravne / regulatorne, ugledne);
- določitev ciljne časovne točke za obnovo procesa (RTO) in ciljne točke obnove podatkov (RPO);
- identifikacijo odvisnosti in navedbo potrebnih virov (osebje, zunanji dobavitelji (pogodbe), infrastruktura);
- navedbo informacijskih sistemov (strojna in programska oprema) in komunikacijskih povezav, ki omogočajo delovanje procesom in
- razvrstitev ključnih procesov na podlagi podane metodologije glede na njihovo kritičnost (pomembnost) in vrstni red obnove glede na skupno oceno kritičnosti procesa (kritični procesi z višjo skupno oceno imajo prednost pri vrstnem redu obnove).

Seznam informacijskih sistemov, ki podpirajo oziroma zagotavljajo delovanje poslovnih procesov oziroma storitev (z označitvijo kritičnih sistemov) je v Prilogi II, ki je sestavni del te politike.

Metodologijo in postopek za izvedbo analize vplivov na poslovanje ter samo izvedbo po poslovnih procesih natančneje določa dokument Analiza vplivov na poslovanje [IME ORGANIZACIJE].

8. Načrt neprekinjenega poslovanja (ang. *Business Continuity Plan - BCP*)

[IME ORGANIZACIJE] izdelava načrt neprekinjenega poslovanja, ki se redno preverja ob upoštevanju politike neprekinjenega poslovanja, rezultatov ocene tveganj in analize vplivov na poslovanje ter ob upoštevanju načela vseh nevarnosti (ang. *All Hazards Approach*).

8.1 Vsebina načrta:

Načrt neprekinjenega poslovanja obsega najmanj:

- postopke za odziv na incidente (npr. požar, izpad IT, kibernetični napadi, naravne nesreče);
- nadomestne lokacije in postopki za preselitev ključnih funkcij;
- komunikacijski načrt z notranjimi in zunanjimi deležniki;
- protokol za interno poročanje in aktivacijo krizne ekipe;
- navodila za obnovo omrežnih in informacijskih sistemov in dostopa do podatkov in
- kontaktni seznam odgovornih oseb, dobaviteljev in podpornega osebja.

7

8.2 Aktivacija načrta:

Načrt se aktivira ob zaznavi dogodka, ki je ali bi lahko povzročil motnjo delovanja. Aktivacijo načrta neprekinjenega poslovanja odobri krizna ekipa ali vodstvo organizacije.

9. Minimalna raven poslovanja

V [IME ORGANIZACIJE] je določena minimalna raven poslovanja, ki obsega nujno potrebne poslovne procese, ki omogočajo delovanje oziroma poslovanje organizacije v izrednih ali kriznih razmerah.

Za vsako ključno funkcijo oziroma **kritičen proces** morajo biti določene minimalne operativne zahteve, ki vključujejo:

- nujno potrebno osebje;
- osnovne informacijske in komunikacijske storitve;
- nujne dobavitelje, partnerje in dobavne poti ter

- potrebne zakonske in varnostne pogoje za delovanje.

Poslovni procesi, ki obsegajo določeno minimalno raven poslovanja so določeni oziroma označeni v Prilogi II, ki je sestavni del te politike.

10. Upravljanje varnostnih kopij in redundantnih zmogljivosti

Organizacija izvaja varnostno kopiranje podatkov in zagotavlja redundantne zmogljivosti in sicer:

- redno izvajanje varnostnih kopij podatkov, vključno s konfiguracijskimi podatki in podatki v oblaku;
- shranjevanje varnostnih kopij na varnih lokacijah, ločenih od glavnega sistema, z ustreznim fizičnim in logičnim nadzorom dostopa;
- redno preverjanje celovitosti varnostnih kopij in testiranje postopkov obnove ter dokumentiranje rezultatov;
- določitev obdobja hrambe varnostnih kopij na podlagi poslovnih in regulativnih zahtev ter rezultatov analize obvladovanja tveganj;
- zagotavljanje zadostnih virov, vključno z omrežnimi in informacijskimi sistemi, opremo, zalogami in usposobljenim osebjem, za ohranjanje delovanja v primeru motenj in
- redno testiranje in posodabljanje redundantnih sistemov ter dokumentiranje rezultatov testiranja.

8

Za izvajanje varnostnega kopiranja in upravljanja varnostnih kopij v skladu s to politiko je zadolžen vodja IT oddelka / pogodbeni partner.

11. Vzdrževanje in izboljševanje

Politika neprekinjenega poslovanja se pregleda najmanj enkrat letno ali ob večjih spremembah ali ob pojavu pomembnih incidentov, ki vplivajo na neprekinjenost poslovanja.

Redno se izvajajo simulacije in vaje, rezultati pa se dokumentirajo. Po vsakem pomembnem incidentu se izvede analiza uspešnosti oziroma učinkovitosti in uvedejo izboljšave. Izvaja se spremljanje skladnosti z zakonodajo in mednarodnimi dobrimi praksami.

Prilogi:

- Priloga 1 (Seznam poslovnih procesov)
- Priloga 2 (Seznam informacijskih sistemov, ki zagotavljajo delovanje poslovnih procesov)



Priloga 1: Seznam poslovnih procesov

Št. procesa	Opis procesa	Lastnik procesa	Kritičnost procesa	Minimalno poslovanje (DA/NE)
P-01	Dobava električne energije / oskrba uporabnikov (nadzor SCADA, razdelilne postaje)	Vodja obratovanja / tehnični direktor	Kritičen	DA
P-02	Upravljanje oskrbe s pitno vodo (črpališča, distribucija, monitoring kakovosti)	Vodja službe	Kritičen	DA
P-03	Upravljanje zdravstvenih storitev (EHR sistem, naročanje pacientov)	Vodja enote IT	Kritičen	DA
P-04	Obravnava plačil in finančnih transakcij	Vodja financ	Pomemben	DA
P-05	Upravljanje s človeškimi viri	Vodja enote HR	Podporen	NE
P-06	Komunikacija s pristojnimi organi in javnostjo (v kriznih razmerah)	Vodja krizne komunikacije / PR	Pomemben	DA
P-07	Podpora uporabnikom / Helpdesk	Vodja enote IT	Podporen	NE
P-08	Upravljanje kibernetске varnosti in nadzora sistemov (SOC, SIEM)	CISO	Kritičen	DA

Priloga 2: Seznam informacijskih sistemov, ki zagotavljajo delovanje poslovnih procesov

Opis sistema	Lastnik sredstva	Podpora kritičnim procesom (DA/NE)
SCADA sistem za nadzor električnih in vodnih naprav	Vodja enote IT / Vodja obratovanja	DA
EHR (Elektronski zdravstveni zapisi)	Direktor zdravstvenega doma / Vodja enote IT	DA
ERP sistem (finančno-računovodski modul, kadrovski modul)	Vodja financ / Vodja enote HR	DA
SIEM	CISO	DA
Helpdesk / Service Desk aplikacija	Vodja enote IT	NE
CRM sistem za upravljanje uporabnikov storitev	Vodja nabave / prodaje	DA
E-poštni in komunikacijski sistem (Exchange / 365, Teams)	Vodja enote IT / Vodja infrastrukture	DA
VPN in dostopni strežniki za oddaljeno delo	CISO / Vodja infrastrukture	DA