REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

NAČRT OBNOVITVE IN PONOVNE VZPOSTAVITVE DELOVANJA OMREŽNIH IN INFORMACIJSKIH SISTEMOV – vzorčna dokumentacija

Različica:	1.0
Datum veljavnosti:	
Avtor:	
Odobril:	

November 2025

Uvodna pojasnila

Ta dokument predstavlja vzorčno predlogo za pripravo dokumenta »Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov« iz 5. točke prvega odstavka 21. člena Zakona o informacijski varnosti (Uradni list RS, št. 40/25; v nadaljevanju: ZInfV-1) in je v skladu s Politiko neprekinjenega poslovanja, Načrtom neprekinjenega poslovanja in Analizo vplivov na poslovanje. 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-1[1].

Dokument je del sistema neprekinjenega poslovanja organizacije in predstavlja operativni dokument, ki se uporablja v primeru večjih motenj ali prekinitve delovanja omrežnih in informacijskih sistemov oziroma ob aktiviranju načrta neprekinjenega poslovanja. Namenjen je predvsem krizni ekipi, ekipi za obnovo IT sistemov ter pogodbenim izvajalcem, ki sodelujejo pri obnovi in ponovni vzpostavitvi delovanja. Dokument dopolnjuje in podrobneje udejanja Politiko neprekinjenega poslovanja ter Načrt neprekinjenega poslovanja in temelji na rezultatih analize vplivov na poslovanje ter ocene tveganj.

Navedeni dokument predstavlja poenostavljen, a za uporabo v praksi usmerjen načrt izvedbe obnovitve in ponovne vzpostavitve nekaterih vzorčnih in naključno izbranih ključnih procesov, ki so odvisni od omrežnih in informacijskih sistemov, ter prehod v normalno delovanje. Osredotoča se izključno na tehnično-informacijske vidike obnove in dopolnjuje širši Načrt neprekinjenega poslovanja, ki obravnava tudi poslovne procese, kadre, prostore in dobavno verigo.

Organizacija lahko dokument neposredno uporabi z upoštevanjem stanja lastne informacijsko-komunikacijske infrastrukture, posebnosti sektorja, obseg in kompleksnosti poslovanja ter ostalih lastnih internih dokumentov sistema upravljanja neprekinjenega poslovanja. Bistvene priloge dokumenta so tudi načrti ponovne vzpostavitve posameznih sistemov oziroma aplikacij, ki pa so strokovno-tehnične narave. Dokument podpiše oziroma odobri vodstvo organizacije in ga najmanj letno pregleda.

<u>Uporabljeni viri</u>:

- *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 tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (Uradni list EU, L 2024/2690);*
- *Standard ISO/IEC 27001:2022;*
- *Standard ISO/IEC 22301:2019;*
- *Strokovni okvir NIST Cybersecurity Framework (CSF);*
- *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 tržnic, 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

Ta dokument določa načrt za obnovitev in ponovno vzpostavitev delovanja omrežnih in informacijskih sistemov [IME ORGANIZACIJE], s poudarkom na hitri in uspešni obnovi po prekinitvah, ki jih povzročijo nepredvideni dogodki ali motnje. Načrt je usklajen s Politiko neprekinjenega poslovanja, Načrtom neprekinjenega poslovanja ter rezultati analize vpliva na poslovanje (BIA) in ocene tveganj.

Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov predstavlja strukturiran pristop [IME ORGANIZACIJE] k ohranjanju in ponovni vzpostavitvi ključnih omrežnih in informacijskih sistemov v primeru incidentov oziroma nepredvidljivih dogodkov, ki povzročijo metne ali prekinitev delovanja ključnih oziroma kritičnih procesov in poslovnih funkcij.

Dokument določa ključne vloge, odgovornosti in postopke za obnovitev, vključno z merljivimi cilji, kot so ciljni čas obnove (RTO) in ciljna točka obnove podatkov (RPO), ter kazalnike uspešnosti za spremljanje uspešnosti.

2. Omejitve pri izvajanju

Tega načrta obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov morda ne bo mogoče izvesti (deloma ali v celoti) v primeru, ko ne bi bilo mogoče – deloma ali v celoti izvajati Načrta neprekinjenega poslovanja.

3. Obseg načrta

Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov obsega:

- vloge in odgovornosti;
- komunikacijske postopke;
- protokol za aktivacijo ekipe za obnovo;
- kontaktni seznam;
- postopke za obnovo ključnih sistemov (vključno z nadomestnimi lokacijami in redundanco);
- protokole za odziv na tipične incidente (npr. izpad strežnikov, kibernetski napadi, požar) in
- obnovo varnostnih kopij ter testiranje obnove.

Obseg vključuje vse omrežne in informacijske sisteme iz Priloge 2 Politike neprekinjenega poslovanja, s fokusom na kritične sisteme.

Za vsak posamezni omrežni in informacijski sistem mora biti na varnem mestu shranjen (tehnični) postopkovnik s posameznimi koraki oziroma opravili za vzpostavitev sistema v normalno delovanje.

4. Vloge in odgovornosti

Funkcija	Odgovornosti
Direktor/predstojnik organizacije	Potrdi načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; s sklepom določi vodjo obnove IT sistemov; s sklepom imenuje ekipo za obnovo IT sistemov; dodeli potrebne vire; zagotovi skladnost z zakonodajo.
Vodja obnove IT sistemov	Skrbi za razvoj, posodabljanje in izvajanje načrta obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; aktivira in koordinira ekipo za obnovo IT sistemov; organizira testiranje načrta; poroča vodstvu.
Krizna ekipa	Aktivira Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov; sodeluje z vodjo obnove IT sistemov; izvaja notranjo komunikacijo.
Ekipa za obnovo IT sistemov	Izvaja aktivnosti za obnovo in ponovno vzpostavitev delovanja IT sistemov; vključuje pogodbene izvajalce; sodeluje pri testiranju načrta.
IT oddelek/pogodbeni izvajalci	Ekipi za obnovo nudi vso potrebno podporo pri izvajanju aktivnosti za obnovitev sistemov.

Vodja obnove omrežnih in informacijskih sistemov je Peter *Novak*.

Ekipo za obnovo omrežnih in informacijskih sistemov sestavljajo: *Peter Novak, Janez Novak in Srečko Kosovel* ter predstavniki pogodbenih izvajalcev: *Areead Goldberg, Henrik Begsteiger.*

5. Kontaktni seznam odgovornih oseb in dobaviteljev[3]

- *Seznam ključnih zaposlenih s kontaktnimi podatki (s telefonskimi številkami, kjer so stalno dosegljivi in e-pošto), funkcijami in zadolžitvami.*
- *Seznam ključnih dobaviteljev z njihovimi storitvami in kontaktnimi podatki.*
- *Dodatni kontakti: ponudniki internetnih storitev, vzdrževalci opreme, zunanji izvajalci.*
- *Redno preverjanje in posodabljanje podatkov.*

6. Postopki za obnovo in ponovno vzpostavitev omrežnih in informacijskih sistemov

V primeru pojava tipičnih scenarijev dogodkov oziroma incidentov, ki povzročijo aktivacijo Načrta obnove in ponovne vzpostavitve omrežnih in informacijskih sistemov se sledi naslednjim standardnim postopkom:

6.1 Požar s prizadetostjo fizične infrastrukture

Za obnovo omrežnih in informacijskih sistemov po požaru, ki poškoduje fizično infrastrukturo (npr. strežnike, podatkovne centre), je pomembna hitra izolacija, preselitev in validacija. Pomembna je alternativna lokacija in obnova iz redundančnih virov, brez splošnih elementov neprekinjenega poslovanja.

[3] Organizacija tekst poglavja izpiše glede na področne posebnosti in dejansko stanje.

1. Ocenitev škode na infrastrukturi: Pregleda se prizadete strežnike, kable in opremo za fizične poškodbe; identificira se kritične sisteme skladno z oceno vpliva na poslovanje in se določi vpliv na podatke (npr. preveri se integriteta diskov).
2. Izvedba izolacije in preklopa na redundančne sisteme: Izklopi se poškodovana oprema iz omrežja; aktivira se »*failover*« na alternativnem mestu (npr. oblak ali sekundarni data center) in se preseli podatke prek varnih kanalov.
3. Izvedba obnove sistemov iz varnostnih kopij: Uporabi se ločene, nepoškodovane kopije za obnovo (npr. restavracija operacijskega sistema, aplikacij in podatkov); izvede se test celovitosti kopij pred izvedbo obnove.
4. Validacija in testiranje obnovljenih sistemov: Preveri se funkcionalnost (npr. dostop do aplikacij, hitrost omrežja); izvede se varnostni pregled za zaznavo morebitnih sekundarnih poškodb.
5. Sinhronizacija in vrnitev v normalno delovanje: Sinhronizirajo se podatki med alternativnim in popravljenim primarnim sistemom; izvedite se polni »*backup*« po obnovi.

6.2 Odpoved ključne strojne opreme

Za obnovo po odpovedi strojne opreme (npr. strežnik, disk), se sledi smernicam, ki poudarjajo redundanco in hitro zamenjavo, s fokusom na IT-specifičnih korakih.

1. Zaznavanje in diagnosticiranje odpovedi: Uporaba monitoring orodja za zaznavo (npr. SMART za diske); ocenitev vpliva na sisteme in podatke (npr. preveritev RAID nivojev).
2. Izoliranje odpovedane opreme: Odklopi iz omrežja, da se prepreči širjenje napake; preklop na redundančne komponente (npr. »*failover*« strežnik).
3. Zamenjava in obnovitev strojne opreme: Namestitev nove opreme (npr. nov disk); obnovitev konfiguracije in podatkov iz varnostnih kopij.
4. Testiranje obnove: Preveritev zmogljivosti in integritete (npr. izvedba stresnega testa); zagotovitev skladnosti z RTO / RPO.
5. Vrnitev v produkcijo: Sinhronizacija z obstoječimi sistemi; dokumentiranje sprememb za prihodnje reference.

6.3 Izpad komunikacij

Za obnovo IT komunikacij (npr. internet, VPN), se upoštevajo najboljše prakse za alternativne kanale in hiter preklop.

1. Zaznavanje izpada: Uporaba monitoringa (npr. »*ping*« testi) za potrditev; ocenitev vpliva na IT storitve (npr. dostop do oblaka).
2. Preklop na alternativne poti: Aktivacija redundančne povezave (npr. mobilni podatki, sekundarni ISP); konfiguracija VPN preko drugega kanala.
3. Obnovitev primarne komunikacije: Kontaktiranje ponudnika za popravek; testiranje obnove (npr. preveritev hitrosti in varnosti).

4. Validacija sistemov: Preveritev dostopa do aplikacij in podatkov; sinhronizacija zamujenih transakcij.
5. Optimizacija za prihodnost: Posodobitev redundance (npr. doda se več ponudnikov); dokumentiranje incidenta.

6.4 Izpad IT storitev

Za obnovo po izpadu IT storitev (npr. aplikacije, oblak), je potrebno slediti postopkov za »*failover*« in obnovo.

1. Zaznavanje in analiza izpada: Uporaba SIEM za zaznavo; ocenitev vzroka (npr. napaka v aplikaciji) in vpliva na sisteme.
2. Izoliranje problema: Zaustavitev širjenja (npr. izklop prizadetega strežnika); preklop na redundančne storitve.
3. Obnovitev iz kopij: Restavracija aplikacije in podatkov iz varnostnih kopij; testiranje funkcionalnosti.
4. Validacija obnove: Preveritev integritete in zmogljivosti; izvedba varnostnega pregleda.
5. Vrnitev v normalno delovanje: Sinhronizacija sistemov; izvedba polnega »*backupa*«.

6.5 Odpoved storitev ključnih pogodbenih izvajalcev (prehod na novega)

Za prehod na novega izvajalca po odpovedi, se upoštevajo najboljše prakse za migracijo in sklenitev nove pogodbe.

1. Ocenitev vpliva odpovedi: Pregled vpliva na IT sisteme (npr. dostop do storitev); identificiranje kritičnih podatkov za prenos.
2. Priprava podatkov za migracijo: Izvoz podatkov in konfiguracije; preveritev skladnosti z SLA starega izvajalca.
3. Aktiviranje novega izvajalca: Podpis pogodbe in SLA; prenos podatkov prek varnih kanalov (npr. API migracija).
4. Testiranje integracije: Validacija nove storitve (npr. testiranje dostopa in zmogljivost); izvedba vzporednega testiranja.
5. Zaključek prehoda: De-aktivacija starega izvajalca; dokumentiranje sprememb in posodobitev pogodbe in SLA.

6.6 Kibernetski napad

Za obnovo po kibernetskem napadu (npr. *ransomware*), je potrebno slediti postopkom za izolacijo, čiščenje in validacijo.

1. Zaznavanje in izoliranje napada: Uporaba SIEM za zaznavo; odklop okuženih sistemov iz omrežja.
2. Analiziranje in odstranitev / izkoreninjenje grožnje: Izvedba forenzične preiskave; odstranitev škodljive kode iz vseh prizadetih sistemov (skeniranje in trajen izbris).

3. Izvedba obnovitve iz čistih kopij: Restavracija sistemov iz varnostnih kopij; preveritev celovitosti pred obnovo.
4. Validacija sistemov: Izvedba testiranja za iskanje morebitnih ostankov grožnje; posodobitev varnosti (npr. namestitev varnostnih popravkov, uvedba MFA).
5. Vrnitev v normalno delovanje: Sinhronizacija podatkov; izvedba post-incident »*backup*« in poročanje CSIRT skupini.

Najprej se poskuša obnoviti delovanje omrežnih in informacijskih sistemov na primarni lokaciji, če je to časovno in operativno najbolj učinkovito. Če se pri tem izkaže, da obnova ne bo uspešna ali bo predolgotrajna, se prične s postopkom vzpostavitve delovanja na nadomestni lokaciji. Odločitev o tem sprejme krizna ekipa v posvetovanju z vodjo obnove IT sistemov.

Za vsak posamezni informacijski sistem ali posamezno sredstvo (npr. usmerjevalnik, stikalo) se izdela Navodilo za obnovo sistema po korakih, ki mora biti varno hranjeno na vsaj dveh različnih lokacijah in biti dostopno vodji obnove IT sistemov, članom krizne ekipe in članom ekipe za obnovo IT sistemov.

Za vsako IT napravo, za katere delovanje je potrebna konfiguracijska datoteka, je potrebno aktualne produkcijske konfiguracijske datoteke hraniti na dveh varnih mestih, ki sta ustrezno oddaljena. Dokumentacija mora biti dostopna vodji obnove IT sistemov, članom krizne ekipe in članom ekipe za obnovo IT sistemov.

7. Aktivacija načrta

Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov se aktivira po zaznavi dogodka, ki je povzročil motnje delovanja bistvenih oziroma ključnih storitev.

Odločitev o aktivaciji Načrta obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov sprejme krizna ekipa.

Krizna ekipa sprejema vse ključne odločitve in izvaja potrebna usklajevanja z vodjo obnove IT sistemov.

8. Vzdrževanje, izboljševanje in testiranje

Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov se pregleda najmanj enkrat letno, ob večjih spremembah ali ob pojavu izrednih dogodkov, ko je bil aktiviran Načrt neprekinjenega poslovanja oziroma Načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov.

Redno se izvajajo in dokumentirajo simulacije ter testiranja. Vsako leto se izvedeta najmanj dve testiranji načrta po dveh različnih tipičnih scenarijih.

Najmanj dvakrat letno se izvede testiranje UPS sistemov rezervnega napajanja in testiranje dizelskih agregatov rezervnega napajanj pod obremenitvijo.

Po vsakem pomembnem incidentu se izvede analiza uspešnosti in uvedejo izboljšave.