| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P15 | | | | | Naslov dokumenta:<br>**Politika varnostnega kopiranja in obnovitve** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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 6.1.3, 8 | Obravnava tveganj, načrtovanje in operativne kontrole varnostnega kopiranja |
| ISO/IEC 27002:2022 | Kontrole 8.13, 5.28, 5 | Upravljanje varnostnih kopij, varno odstranjevanje |
| NIST SP 800-53 Rev.5 | CP-9, CP-10, SI-12, MP-6 | Zahteve glede varnostnega kopiranja sistemov, obnovitve in sanitizacije medijev |
| Uredba EU GDPR | Člen 32, uvodna izjava 49 | Obnovitev in razpoložljivost osebnih podatkov, neprekinjeno poslovanje |
| Direktiva EU NIS2 | Člen 21(2)(c-e) | Kontrole varnostnega kopiranja in neprekinjenega poslovanja za odpornost |
| Uredba EU DORA | Člena 10, 11 | Zahteve finančnega sektorja glede varnostnega kopiranja, obnovitve in testiranja |
| COBIT 2019 | DSS01, DSS04, MEA | Operacije varnostnega kopiranja, neprekinjeno poslovanje in spremljanje skladnosti |

## 1. Namen

1.1 Namen te politike je določiti obvezne zahteve za varnostno kopiranje in obnovitev podatkov, sistemov in aplikacij za podporo operativni odpornosti, celovitosti podatkov in neprekinjenemu poslovanju.

**1.2 Ta politika vzpostavlja standardiziran okvir za:**

1.2.1 zaščito podatkov organizacije pred izgubo zaradi izbrisa, okvare podatkov, odpovedi sistema ali kibernetskih napadov

1.2.2 opredelitev pričakovanj glede obnovitve z jasno določenima parametroma RTO (ciljni čas obnovitve) in RPO (ciljna točka obnovitve)

1.2.3 vključitev postopkov varnostnega kopiranja v širši sistem upravljanja informacijske varnosti (ISMS) in načrte neprekinjenega poslovanja (BCP/DRP)

1.2.4 zagotavljanje skladnosti z veljavnimi zakoni in sektorskimi predpisi glede razpoložljivosti in obnovljivosti

1.3 Ta politika uvaja kontrole standarda ISO/IEC 27001:2022, povezane z varnim odstranjevanjem podatkov (5.28), odpornostjo (5.29) in operativno obnovitvijo (8.13), ter se sklicuje na dobre prakse iz ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA in NIS2.

## 2. Področje uporabe

**2.1 Ta politika se uporablja za:**

2.1.1 vse poslovno kritične in operativne sisteme v obsegu ISMS

2.1.2 vse strukturirane in nestrukturirane poslovne podatke, vključno s podatkovnimi zbirkami, datotekami, e-pošto in konfiguracijami

2.1.3 vsa okolja – v lastnih prostorih, v oblaku, hibridna ter oddaljene lokacije/shranjevanje izven lokacije

2.1.4 vse osebe, odgovorne za upravljanje, izvajanje, preverjanje ali obnovitev procesov varnostnega kopiranja

**2.2 Prav tako se uporablja za:**

2.2.1 medije in infrastrukturo za varnostno kopiranje, vključno s fizičnimi trakovi, virtualnimi napravami, posnetki diskov in rešitvami za varnostno kopiranje v oblaku

2.2.2 zunanje ponudnike, pogodbeno vključene za gostovanje, upravljanje ali obdelavo varnostnih kopij organizacije

2.2.3 varnostno kopiranje dnevnikov, konfiguracij, revizijskih sledi in operativne dokumentacije, ključne za neprekinjeno poslovanje

2.3 Sistemi, ki so izrecno izključeni iz varnostnega kopiranja, morajo biti dokumentirani, predmet ocene tveganja in formalno odobreni s strani vodje ISMS in lastnika sistema.

**3. Cilji**

3.1 Zagotoviti, da se vsi ključni sistemi in podatki zanesljivo varnostno kopirajo z ustrezno pogostostjo, redundanco in varnostnimi kontrolami.

3.2 Zagotoviti mehanizme za obnovitev, ki izpolnjujejo opredeljena pričakovanja glede RTO in RPO v skladu z analizami vpliva na poslovanje.

3.3 Vzdrževati popolno dokumentacijo postopkov varnostnega kopiranja, rokov hrambe, vlog in tehnologij.

3.4 Potrjevati učinkovitost postopkov varnostnega kopiranja s sistematičnim testiranjem obnovitve, beleženjem odpovedi in spremljanjem odprave pomanjkljivosti.

3.5 Zaščititi podatke varnostnih kopij pred nepooblaščenim dostopom, spremembo ali uničenjem v celotnem njihovem življenjskem ciklu.

**3.6 Omogočiti skladnost z:**

3.6.1 zahtevami standarda ISO/IEC 27001 glede operativnih kontrol in neprekinjenega poslovanja

3.6.2 družinami kontrol NIST SP 800-53 CP in MP za varnostno kopiranje in sanitizacijo

3.6.3 členom 32 in uvodno izjavo 49 GDPR glede obnovitve dostopa do osebnih podatkov

3.6.4 členom 10 DORA in členom 21 NIS2 glede neprekinjenega poslovanja in odpornosti sistemov IKT

3.7 Zagotoviti, da storitve varnostnega kopiranja zunanjih ponudnikov izpolnjujejo pogodbene in regulativne varnostne obveznosti, vključno s šifriranjem, odstranjevanjem in protokoli obveščanja.

**4. Vloge in odgovornosti**

**4.1 Najvišje vodstvo**

4.1.1 Potrdi to politiko in zagotovi, da so poslovno kritični sistemi ustrezno zaščiteni z odobrenimi praksami varnostnega kopiranja in obnovitve.

4.1.2 Odgovarja za to, da so postopki varnostnega kopiranja ustrezno kadrovsko in tehnično podprti ter redno pregledovani z vidika regulativne skladnosti.

**4.2 Vodja informacijske varnosti (CISO)**

4.2.1 Je lastnik te politike in zagotavlja usklajenost s širšimi okviri informacijske varnosti, upravljanja tveganj in neprekinjenega poslovanja.

4.2.2 Nadzira vključevanje postopkov varnostnega kopiranja v BCP/DRP, odzivanje na incidente in načrtovanje odpornosti.

4.2.3 Pregleduje izjeme pri varnostnem kopiranju in ocenjuje predloge za sprejem tveganja pri izključitvah ključnih sistemov.

[ ... 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 Ta politika se mora pregledati najmanj enkrat letno ali prej, če to sprožijo:**

9.1.1 spremembe strategije neprekinjenega poslovanja ali obnovitve po nesreči

9.1.2 nove regulativne ali pravne obveznosti, ki vplivajo na pogostost varnostnega kopiranja ali hrambo podatkov

9.1.3 spremembe sistemske arhitekture, orodij za varnostno kopiranje ali ponudnikov storitev

9.1.4 pomembni incidenti ali ugotovitve presoje, povezani z izgubo podatkov ali neuspešno obnovitvijo

**9.2 Pregled usklajuje vodja informacijske varnosti (CISO) v sodelovanju z:**

9.2.1 skupino za infrastrukturo in IT-operacije

9.2.2 notranjo revizijo

9.2.3 pooblaščeno osebo za varstvo podatkov (DPO)

9.2.4 skupinami za neprekinjeno poslovanje in obnovitev po nesreči

**9.3 Urniki varnostnega kopiranja, seznami vključenih sistemov, dokumentacija obnovitve in dnevniki izjem se morajo pregledovati vzporedno, da se zagotovi:**

9.3.1 točnost pokritosti varnostnega kopiranja za vsa ključna sredstva

9.3.2 skladnost z zahtevami RTO/RPO in hrambe

9.3.3 popolnost dnevnikov testiranj in poročil o incidentih

9.3.4 odprava predhodno ugotovljenih kontrolnih vrzeli

**9.4 Vse posodobitve morajo:**

9.4.1 biti verzionirane in hranjene v repozitoriju dokumentacije ISMS

9.4.2 vključevati povzetek sprememb in utemeljitev

9.4.3 biti odobrene s strani najvišjega vodstva

9.4.4 biti sporočene vsem prizadetim tehničnim in poslovnim deležnikom

**10. Povezane politike in povezave**

**10.1 Ta politika neposredno podpira in se povezuje z naslednjimi dokumenti:**

10.1.1 P6 - Politika upravljanja tveganj: določa prednostno obravnavo zaščite varnostnega kopiranja sistemov in storitev na podlagi tveganj.

10.1.2 P12 - Politika upravljanja sredstev: zagotavlja, da so sistemi, primerni za varnostno kopiranje, vključeni v popis sredstev ter povezani s sledenjem življenjskega cikla in klasifikacijo.

10.1.3 P13 - Politika klasifikacije in označevanja podatkov: usmerja, katere kategorije podatkov zahtevajo varnostno kopiranje, vključno z metapodatki za označevanje zaradi določanja prioritet.

10.1.4 P14 - Politika hrambe podatkov in odstranjevanja: usklajuje hrambo varnostnih kopij z regulativnimi omejitvami hrambe in pravilnim odstranjevanjem medijev po izteku roka.

10.1.5 P16 - Politika maskiranja podatkov in psevdonimizacije: podpira minimizacijo podatkov pri varnostnem kopiranju občutljivih naborov podatkov.

10.1.6 P30 - Politika odzivanja na incidente: aktivira se ob odpovedih varnostnega kopiranja, težavah pri obnovitvi ali kompromitaciji repozitorijev podatkov varnostnih kopij.

10.2 Te medsebojno povezane politike tvorijo skladen okvir, ki zagotavlja, da je upravljanje varnostnega kopiranja vključeno v širši ISMS organizacije in strategijo operativne odpornosti.

## 11. Referenčni standardi in okviri

### 11.1 ISO/IEC 27001:

11.1.1 Klavzula 6.1.3 - načrt obravnave tveganj: podpira določanje prioritet varnostnega kopiranja in načrtovanje obnovitve na podlagi tveganj.

11.1.2 Klavzula 8.1 - operativno načrtovanje in nadzor: vključuje kontrole obnovitve in neprekinjenega poslovanja kot del operativnih varovalnih ukrepov.

11.1.3 Kontrola 5.28 iz Priloge A - varno odstranjevanje ali ponovna uporaba opreme: obravnava varno sanitizacijo medijev za varnostne kopije.

11.1.4 Kontrola 5.29 iz Priloge A - informacijska varnost med motnjo: zagotavlja zmožnosti obnovitve med incidenti ali nesrečami.

11.1.5 Kontrola 8.13 iz Priloge A - varnostno kopiranje informacij: neposredno obravnavana z načrtovanimi, testiranimi in varnimi operacijami varnostnega kopiranja.

11.2 ISO/IEC 27002:2022 - Kontrole 8.13, 5.28, 5: Te kontrole krepijo zahtevo po rednem varnostnem kopiranju, preverjanju celovitosti in načrtovanju obnovitve v vseh IT-okoljih.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - varnostno kopiranje sistema: vzpostavlja celovite postopke varnostnega kopiranja, vključno s shranjevanjem izven lokacije in testiranjem obnovitve.

11.3.2 CP-10 - obnovitev in povrnitev sistema: zahteva potrjene postopke za popolno ali delno obnovitev, usklajene s cilji obnovitve.

11.3.3 MP-6 - sanitizacija medijev: zagotavlja varno ravnanje z zastarelimi mediji za varnostne kopije.

11.3.4 SI-12 - postopki ravnanja z informacijami: krepi odgovornosti glede varnostnega kopiranja in obnovitve za občutljive podatke.

### 11.4 Uredba EU GDPR (2016/679):

11.4.1 Člen 32 - varnost obdelave: zahteva zmožnosti obnovitve in varovalne ukrepe za razpoložljivost podatkov, zlasti osebnih podatkov.

11.4.2 Uvodna izjava 49: podpira ukrepe neprekinjenega poslovanja in obnovitve po nesreči, vključno z varnim varnostnim kopiranjem kot delom organizacijske odpornosti.

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

11.5.1 Člen 21(2)(c-e): zahteva tehnične in organizacijske ukrepe, vključno s kontrolami varnostnega kopiranja in neprekinjenega poslovanja, za zagotavljanje odpornosti storitev.

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

11.6.1 Člen 10 - IKT neprekinjeno poslovanje: zahteva, da imajo finančni subjekti celovito varnostno kopiranje podatkov, obnovitev in načrtovanje neprekinjenega poslovanja.

11.6.2 Člen 11 - testiranje načrtov IKT za neprekinjeno poslovanje: poudarja potrjevanje zmožnosti obnovitve z rednim testiranjem.

### 11.7 COBIT 2019:

11.7.1 DSS01 - upravljane operacije: podpira zanesljivo izvajanje storitev z zaščiteno razpoložljivostjo podatkov.

11.7.2 DSS04 - upravljana neprekinjenost: opredeljuje strateške in operativne kontrole neprekinjenega poslovanja, vključno s preverjenimi varnostnimi kopijami.

11.7.3 MEA03 - spremljanje, vrednotenje in ocenjevanje skladnosti: zahteva periodični pregled ukrepov neprekinjenega poslovanja, vključno z učinkovitostjo kontrol varnostnega kopiranja.