REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
Twitter: @URSIV_Slovenia

| |
|---|
| Številka: 007-13/2022/53 |
| Ljubljana, 30. 8. 2023 |
| EVA: 2022-1544-0004 |
| GENERALNI SEKRETARIAT VLADE<br>REPUBLIKE SLOVENIJE |

**ZADEVA: Predlog Uredbe o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave – predlog za obravnavo**

**1. Predlog sklepov vlade:**

Na podlagi tretjega odstavka 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23-ZDU-1O in 49/23) je Vlada Republike Slovenije na … seji … sprejela

SKLEP

Vlada Republike Slovenije je izdala Uredbo o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave ter jo objavi v Uradnem listu Republike Slovenije.

Barbara Kolenko Helbl
generalna sekretarka

Sklep prejmejo:
- Urad Vlade Republike Slovenije za informacijsko varnost,
- vsa ministrstva in vladne službe.

Prilogi:

– predlog Uredbe o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave,
– obrazložitev uredbe.

**2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:**

/

**3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:**

- Dr. Uroš Svete, direktor urada, Urad Vlade Republike Slovenije za informacijsko varnost
- Kory Golob, pomočnik direktorja urada, Urad Vlade Republike Slovenije za informacijsko varnost

- Barbara Pernuš Grošelj, sekretarka, Služba direktorja urada, Urad Vlade Republike Slovenije za informacijsko varnost

**3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:**

/

**4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:**

/

**5. Kratek povzetek gradiva:**

Predlog uredbe o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (v nadaljnjem besedilu predlog uredbe) se izdaja v skladu z Zakonom o spremembah in dopolnitvi Zakona o informacijski varnosti (Uradni list RS, št. 95/21; v nadaljnjem besedilu ZInfV-A). Po prehodni določbi 13. člena ZInfV-A je namreč z dnem uveljavitve ZInfV-A prenehal veljati (tudi) Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19; v nadaljnjem besedilu pravilnik), ki pa se uporablja do izdaje podzakonskih predpisov iz drugega odstavka prejšnjega člena ZInfV-A (torej 12. člena ZInfV-A). Ob tem je treba pojasniti, da je ZInfV-A, posegel v osnovni Zakon o informacijski varnosti (Uradni list RS, št. 30/18) med drugim tudi v tretji odstavek 17. člena, kjer je besedilo »Minister« nadomestil z besedo »Vlada«. S tem je bila z ZInfV-A spremenjena pristojnost za izdajo podzakonskega predpisa, ki ureja varnostno dokumentacijo in varnostne ukrepe organov državne uprave, pri čemer je navedena pristojnost prešla iz dotlej resorno pristojnega ministra (ki je izdal pravilnik) na Vlado Republike Slovenije (v nadaljnjem besedilu vlada).

Predlog uredbe v največji meri ohranja dosedanjo vsebino pravilnika, ki je namenjena organom državne uprave, ki so kategorija zavezancev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23-ZDU-1O in 49/23; v nadaljnjem besedilu ZInfV). Pri tem so po 3. alineji prvega odstavka 5. člena ZInfV zavezanci tisti organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljnjem besedilu: organi državne uprave). Pri tem posamične zavezane organe državne uprave določi vlada na podlagi prvega odstavka 9. člena (določitev organov državne uprave) ZInfV. Vsebinska ureditev predlagane uredbe se glede na ureditev pravilnika spreminja in dopolnjuje le v manjšem obsegu in sicer glede na pomanjkljivosti ureditve pravilnika, kot so bile zaznane pri njegovem izvajanju v praksi in sicer predvsem v postopkih nadzora. Namen vsebinskih sprememb je dosedanjo ureditev dodatno izboljšati na način, da bo za uporabnike oziroma naslovljence tega predpisa bolj jasna in lažja za uporabo ter hkrati preglednejša za potrebe kasnejšega nadzora s strani pristojnega inšpektorja. Predlogi izboljšav vsebinske ureditve v predlagani uredbi glede na pravilnik so omejeni glede na možnosti oziroma vsebino veljavnega ZInfV. Večje spremembe relevantne podzakonske ureditve bodo možne šele po sprejemu novega sistemskega zakona (t.i. ZInfV-1), kar pa bo treba že zaradi prenosa nove horizontalne direktive Evropske unije (EU) s področja varnosti omrežnih in informacijskih sistemov v slovenski pravni red, pri čemer gre za Direktivo (EU) 2022/2555 (direktiva NIS 2) (UL L št. 333 z dne 27. 12. 2022, str. 80) z rokom za prenos 17. 10. 2024.

Spreminja se oblika predpisa, ki je po ZInfV-A uredba, ki jo izda vlada. Z izdajo predlagane uredbe se torej upošteva načelo pravne države.

**6. Presoja posledic za:**

| | | |
|---|---|---|
| a) | javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih | NE |
| b) | usklajenost slovenskega pravnega reda s pravnim redom Evropske unije | NE |
| c) | administrativne posledice | NE |
| č) | gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij | NE |
| d) | okolje, vključno s prostorskimi in varstvenimi vidiki | NE |
| e) | socialno področje | NE |

| | | |
|---|---|---|
| f) | dokumente razvojnega načrtovanja:<br>– nacionalne dokumente razvojnega načrtovanja<br>– razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna<br>– razvojne dokumente Evropske unije in mednarodnih organizacij | NE |

**7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:**

/

**I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu**

| | Tekoče leto (t) | t + 1 | t + 2 | t + 3 |
|---|---|---|---|---|
| Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna | | | | |
| Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov | | | | |
| Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna | | | | |
| Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov | | | | |
| Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva | | | | |

**II. Finančne posledice za državni proračun**

**II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:**

| Ime proračunskega uporabnika | Šifra in naziv ukrepa, projekta | Šifra in naziv proračunske postavke | Znesek za tekoče leto (t) | Znesek za t + 1 |
|---|---|---|---|---|
| | | | | |
| **SKUPAJ** | | | | |

**II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:**

| Ime proračunskega uporabnika | Šifra in naziv ukrepa, projekta | Šifra in naziv proračunske postavke | Znesek za tekoče leto (t) | Znesek za t + 1 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| **SKUPAJ** | | | | |

**II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:**

| Novi prihodki | Znesek za tekoče leto (t) | Znesek za t + 1 |
|---|---|---|
| | | |
| | | |
| | | |
| **SKUPAJ** | | |

**OBRAZLOŽITEV:**

**I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu**

/

**II. Finančne posledice za državni proračun**

/

**II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:**

/

**II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:**

/

**II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:**

/

**7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:**

/

**8. Predstavitev sodelovanja z združenji občin:**

| | |
|---|---|
| Vsebina predloženega gradiva (predpisa) vpliva na:<br>- pristojnosti občin,<br>- delovanje občin,<br>- financiranje občin. | NE |

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: NE
- Združenju občin Slovenije ZOS: NE
- Združenju mestnih občin Slovenije ZMOS: NE

Bistveni predlogi in pripombe, ki niso bili upoštevani.

| **9. Predstavitev sodelovanja javnosti:** | |
|---|---|
| Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja: | DA |
| Gradivo ni takšne narave, da bi ga bilo treba objaviti na spletni strani predlagatelja. | |
| *(Če je odgovor DA, navedite:)* | |
| *Datum objave: objava na spletnih straneh e-demokracija dne 13. 6. 2022 z rokom za komentiranje oz. odziv javnosti do 13. 7. 2022. Po ZInfV zavezani organi državne uprave so bili o tej objavi in možnosti komentiranja na e-demokraciji še dodatno pisno obveščeni.*<br><br>*Upoštevani so bili: /*<br>– *v celoti,*<br>– *večinoma,*<br>– ***delno,***<br>– *niso bili upoštevani.*<br><br>*Bistvena mnenja, predlogi in pripombe, ki niso bili upoštevani, ter razlogi za neupoštevanje:*<br><br>- *Predlog (anonimni) za izvedbo anonimne prijave incidenta informacijske varnosti, vključno s predlogom obrazca v predlagani uredbi, ni bil upoštevan, saj gre za zakonsko materijo. Veljavni Zakon o informacijski varnosti (ZInfV) ureja zgolj obveznost prijave incidentov s strani zavezancev in sicer le tistih incidentov, ki imajo pomemben vpliv na neprekinjeno izvajanje njihovih storitev. ZInfV ureja tudi prostovoljno prijavo incidentov s strani subjektov, ki niso bili določeni kot zavezanci po tem zakonu, če imajo incidenti pomemben vpliv na neprekinjeno izvajanje storitev, ki jih ti subjekti zagotavljajo, pri čemer ZInfV ureja tudi vrstni red oziroma možnost obdelave takšnih priglasitev s strani pristojnih CSIRT (nacionalni CSIRT ali CSIRT organov državne uprave). Ob tem je treba še pojasniti, da je prijavo domnevnih kršitev ZInfV (vključno z morebitno kršitvijo obveznosti zavezancev glede poročanja o incidentih) v skladu z Zakonom o inšpekcijskem nadzoru (ZIN) možno podati tudi anonimno. Pri tem je za kršitve ZInfV pristojna Inšpekcija za informacijsko varnost, ki deluje znotraj Urada Vlade Republike Slovenije za informacijsko varnosti (URSIV), v postopku nadzora pa se upoštevajo določbe ZInfV, kot tudi ZIN. Kolikor pa gre za povezavo s prijavo kršitev v delovnem okolju prijavitelja, pa ustrezne poti za prijavo (notranje in zunanje) ter zaščito prijaviteljev ureja Zakon o zaščiti prijaviteljev (Uradni list RS, št. 16/23).*<br>- *Komentarja ali predloga iz spletnih strani e-demokracija z dne 7. 7. 2022 sta bila očitno pomotoma podana pri predlogu tega predpisa, saj sta se vsebinsko nanašala na drug predlog predpisa in sicer na predlog Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, EVA 2022-1544-0003. Zato sta oba predmetna komentarja za vsebino predloga obravnavne uredbe brezpredmetna. Ne glede na navedeno sta bila na oba komentarja zainteresirani osebi, ki ju je podala, že podana pisna pojasnila in sicer z dopisom št. 007-13/2022/24, z dne 18. 1. 2023 in z dopisom št. 007-* | |

| | |
|---|---|
| *13/2022/25, prav tako z dne 18. 1. 2023. Oba pojasnila sta bila glede na vsebino komentarja podana z vidika predloga Uredbe o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, ki jo je Vlada Republike Slovenije medtem tudi že izdala in je bila objavljena v Uradnem listu Republike Slovenije, št. 8/2023 z dne 23. 1. 2023.*<br>- *Pripomba Agencije Republike Slovenije za javnopravne evidence in storitve (AJPES) k tretjemu odstavku 3. člena (takrat še) osnutka predlagane uredbe je bila upoštevna glede opozorila, da mora na tem mestu pisati uredba in ne pravilnik. Ni pa bil upoštevan predlog, naj se ta določba umesti med prehodne in končne določbe ali celo izbriše, zaradi izogibanja ponavljanja napotil za uskladitev notranjih aktov na dveh ločenih segmentih uredbe. Glede na vsebino določbe tretjega odstavka 3. člena predlagane uredbe (»Če ima ODU za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni v skladu s to uredbo.«) gre namreč za materialno in ne za prehodno določbo, ki je hkrati tudi primerljiva s četrtim odstavkom 17. člena ZInfV. (»Če ima organ državne uprave za zagotavljanje varnosti sovjih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo dopolni skladno s tem zakonom«). Določba 12. člena predlagane uredbe pa ureja prehodno obdobje. Ob tem tudi Služba Vlade Republike Slovenije za zakonodajo (SVZ) ni dala takšne pripombe. Upoštevani pa sta bili še pripombi AJPES k prvi alineji 9. člena in k napovednemu stavku 11. člena (takrat še) osnutka predlagane uredbe, da gre za uredbo in ne pravilnik.*<br><br>*Poročilo je bilo dano ……...* | |
| **10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:** | DA |
| **11. Gradivo je uvrščeno v delovni program vlade:** | NE |
| Dr. Uroš Svete<br><br>direktor urada | |

PRILOGA

Na podlagi tretjega odstavka 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) Vlada Republike Slovenije izdaja

# U R E D B O

## o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave

## I. SPLOŠNE DOLOČBE

### 1. člen
### (vsebina)

Ta uredba podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologijo za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja in pripadajočih podatkov ter minimalni obseg in vsebino varnostnih ukrepov organov državne uprave.

### 2. člen
### (pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. Celovitost je lastnost informacij, omrežij in informacijskih sistemov, da so točni in popolni.
2. Kazalnik zlorabe je kazalnik, ki da informacijo o lastnostih zlorabe omrežij oziroma informacijskih sistemov organov državne uprave (v nadaljnjem besedilu: ODU).
3. Ključni, krmilni in nadzorni informacijski sistemi in deli omrežja ter pripadajoči podatki so informacijski sistemi in deli omrežja ter pripadajoči podatki ODU, ki so bistvenega pomena za delovanje storitev ODU.
4. Neprekinjeno poslovanje so aktivnosti, ki so potrebne za ohranjanje poslovanja organizacije v času motenj ali prekinitev normalnega delovanja.
5. Razpoložljivost je lastnost informacij, omrežij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo.
6. Sistem upravljanja neprekinjenega poslovanja (v nadaljnjem besedilu: SUNP) je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se nanje odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni, ter vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov.
7. Sistem upravljanja varovanja informacij (v nadaljnjem besedilu: SUVI) je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov.
8. Sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za ODU in zato zahteva zaščito.
9. Trajanje incidenta je časovno obdobje od prekinitve ustreznega zagotavljanja storitve v smislu zaupnosti, celovitosti ali razpoložljivosti do trenutka njene ponovne vzpostavitve.
10. Uporabnik je fizična ali pravna oseba, ki uporablja posamezno storitev ODU neposredno, posredno ali s posredovanjem oziroma je odvisna od nje.
11. Zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom.

## II. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

**3. člen**
**(vsebina in struktura varnostne dokumentacije)**

(1) ODU vzpostavijo in vzdržujejo dokumentirana SUVI in SUNP, ki morata zajemati najmanj elemente iz prvega odstavka 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23).

(2) Varnostno dokumentacijo iz prejšnjega odstavka tega člena podpiše predstojnik ODU.

(3) Če ima ODU za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni v skladu s to uredbo.

**4. člen**
**(analiza obvladovanja tveganj)**

Analiza obvladovanja tveganj z določitvijo sprejemljive ravni tveganj, (v nadaljnjem besedilu: analiza obvladovanja tveganj) zajema najmanj:

1. navedbo uporabljene metodologije za izvedbo analize obvladovanja tveganj, ki mora biti primerljiva, verodostojna in ponovljiva v skladu s pravili stroke,
2. navedbo sredstev znotraj SUVI in upravljavce teh sredstev oziroma odgovorne osebe za ta sredstva,
3. navedbo možnih groženj tem sredstvom,
4. navedbo ranljivosti sredstev iz 2. točke tega člena, ki bi jih grožnje iz prejšnje točke lahko prizadele,
5. navedbo vpliva uresničitve groženj iz 3. točke tega člena na zaupnost, celovitost in razpoložljivost sredstev iz 2. točke tega člena zaradi ranljivosti iz prejšnje točke,
6. oceno vpliva na opravljanje storitev ODU v primeru kršitve informacijske varnosti zaradi izgube zaupnosti, celovitosti ali razpoložljivosti,
7. oceno verjetnosti, da nastane kršitev informacijske varnosti,
8. ovrednotenje ravni tveganj,
9. določitev in obrazložitev sprejemljive ravni tveganj,
10. navedbo ukrepov za odpravo ali zmanjšanje tveganj nad sprejemljivo ravnjo.

**5. člen**
**(politika neprekinjenega poslovanja)**

Politika neprekinjenega poslovanja z načrtom njegovega upravljanja zajema najmanj:

1. navedbo ciljev in načel za zagotavljanje neprekinjenega poslovanja ob upoštevanju posebnosti ODU,
2. navedbo postopkov neprekinjenega poslovanja, ki se izdelajo na podlagi popisa poslovnih procesov,
3. oceno vpliva na poslovanje, ki zajema navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije znotraj ODU in odpovedi storitev pogodbenih izvajalcev,
4. določitev minimalne ravni poslovanja,
5. navedbo ukrepov za zagotavljanje neprekinjenega poslovanja, ki se izdelajo na podlagi ocene vpliva na poslovanje iz 3. točke tega člena in minimalne ravni poslovanja iz prejšnje točke, ter
6. določitev vlog in odgovornosti za izvajanje politike neprekinjenega poslovanja ter njeno posodabljanje.

**6. člen**
**(seznam ključnih, krmilnih in nadzornih informacijskih sistemov)**

Seznam informacijskih sistemov in delov omrežja ODU ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev ODU, zajema najmanj:

– navedbo sredstev znotraj SUVI, od katerih je odvisno zagotavljanje storitev ODU, in

– seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov (v nadaljnjem besedilu: ključni sistemi) in navedbo njihovih upravljavcev.

**7. člen**
**(načrt obnovitve delovanja ključnih sistemov)**

Načrt obnovitve in ponovne vzpostavitve delovanja ključnih sistemov iz prejšnjega člena (v nadaljnjem besedilu: načrt obnovitve delovanja ključnih sistemov) zajema opis odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

**8. člen**
**(načrt odzivanja na incidente)**

(1) Načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave (v nadaljnjem besedilu: načrt odzivanja na incidente) zajema najmanj:
1. opis sistema za zaznavo incidentov informacijske varnosti,
2. opis sistema za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo,
3. opis postopkov za odziv na incidente informacijske varnosti, za obravnavo in analizo incidentov informacijske varnosti, vključno z evidentiranjem vseh odzivnih aktivnosti,
4. opis odgovornosti oseb oziroma organizacijskih enot, ki jih je treba vključiti v aktivnosti iz prejšnje točke,
5. opis postopkov in odgovornosti za poročanje o incidentih znotraj ODU in zunaj ODU ter
6. opis protokola obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave.

(2) Obvestilo iz 6. točke prejšnjega odstavka se pošlje CSIRT organov državne uprave na način, ki je objavljen na njegovi spletni strani in zajema najmanj:
1. oceno števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvenih storitev,
2. oceno trajanja incidenta,
3. navedbo kazalnikov zlorabe, če ti obstajajo,
4. oceno geografske razširjenosti območja, na katero incident vpliva,
5. oceno morebitnega medresorskega vpliva incidenta in
6. opis pomembnosti vpliva incidenta na neprekinjeno izvajanje storitev ODU.

(3) Opis protokola obveščanja iz 6. točke prvega odstavka tega člena se lahko smiselno uporabi za obveščanje pristojnega nacionalnega organa za informacijsko varnost, če ima ODU lastne zmogljivosti vsaj na ravni varnostno-operativnega centra.

**9. člen**
**(načrt varnostnih ukrepov)**

(1) Pri izdelavi načrta varnostnih ukrepov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežja in informacijskih sistemov ODU upoštevajo:
– dokumente varnostne dokumentacije iz 3. do 8. člena te uredbe in
– posebne potrebe delovnega področja ODU.

(2) Načrt varnostnih ukrepov iz prejšnjega odstavka vsebuje navedbo ukrepov, ki so:
1. učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje,
2. prilagojeni tako, da se prizadevanja ODU usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost, in se izogibajo podvajanjem,
3. skladni tako, da se prednostno obravnavajo osnovne in skupne varnostne ranljivosti ODU, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna delovna področja,
4. sorazmerni s tveganji tako, da se izogiba čezmerni obremenitvi posameznega ODU,
5. konkretni tako, da ODU te varnostne ukrepe izvajajo in da ti ukrepi prispevajo h krepitvi njihove informacijske varnosti,
6. preverljivi tako, da se na zahtevo pristojnega organa lahko predložijo dokazila o njihovi izvedbi,

7. vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sistemov.

## III. METODOLOGIJI ZA PRIPRAVO ANALIZE OBVLADOVANJA TVEGANJ IN ZA DOLOČITEV KLJUČNIH SISTEMOV

### 10. člen
### (metodologiji za pripravo analize obvladovanja tveganj in za določitev ključnih sistemov)

(1) ODU analizo obvladovanja tveganj pripravi tako, da:
1. navede metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedel analizo obvladovanja tveganj v skladu s to uredbo,
2. izvede popis sredstev znotraj SUVI in določi njihove upravljavce oziroma odgovorne osebe za ta sredstva,
3. prepozna možne grožnje za izgubo zaupnosti, celovitosti in razpoložljivosti sredstev iz prejšnje točke,
4. prepozna ranljivosti sredstev iz 2. točke tega odstavka, ki bi jih grožnje iz prejšnje točke lahko prizadele,
5. oceni stopnjo vpliva uresničitve groženj iz 3. točke tega odstavka na zaupnost, celovitost in razpoložljivost sredstev iz 2. točke tega odstavka zaradi ranljivosti iz prejšnje točke,
6. oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi,
7. ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev ter
8. določi sprejemljivo raven tveganj, glede na vrednotenje ugotovljenih tveganj.

(2) ODU seznam svojih ključnih sistemov pripravi tako, da:
- na podlagi popisanih sredstev znotraj SUVI iz 2. točke prejšnjega odstavka presodi, ali je zagotavljanje storitev ODU odvisno od posameznega sredstva znotraj SUVI, in
- na podlagi posameznih sredstev znotraj SUVI, od katerih je v skladu s prejšnjo alinejo odvisno zagotavljanje storitev ODU, presodi, katero od teh sredstev je bistveno za delovanje storitve ODU.

(3) ODU izvede analizo obvladovanja tveganj ter določi ključne sisteme tako, da bodo rezultati teh postopkov dosledni, primerljivi in verodostojni.

(4) ODU izvaja analizo obvladovanja tveganj in določa ključne sisteme v rednih časovnih presledkih ali kadar so predlagane ali nastanejo bistvene spremembe v okviru SUVI.

## IV. MINIMALNI OBSEG IN VSEBINA VARNOSTNIH UKREPOV

### 11. člen
### (minimalni obseg in vsebina varnostnih ukrepov)

ODU za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežij in informacijskih sistemov na podlagi varnostne dokumentacije iz 3. člena te uredbe pripravijo ter izvajajo organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki zagotavljajo najmanj:
1. podporo predstojnika ODU pri zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni program dela ODU,
2. integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve,
3. notranji pregled SUVI in SUNP najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov,
4. upravljanje ključnih sistemov z določitvijo odgovornosti za njihovo zaščito,
5. ohranjanje dnevniških zapisov o delovanju ključnih sistemov iz prejšnje točke,
6. upravljanje prometa in komunikacij,
7. opredelitev varnostnih zahtev za ključne dobavitelje,
8. fizično in tehnično varovanje dostopov do prostorov, kjer so ključni sistemi,

9. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti ODU,
10. preverjanje identitete uporabnikov,
11. upravljanje in preprečevanje izrabe tehničnih ranljivosti,
12. zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop,
13. zaščito pred zlonamerno programsko kodo,
14. evidentiranje dejavnosti ključnih sistemov, njihovih uporabnikov in administratorjev ter
15. zaznavanje poskusov vdorov in preprečevanje incidentov.

## V. PREHODNI IN KONČNA DOLOČBA

### 12. člen
### (prehodno obdobje)

ODU že izdelano varnostno dokumentacijo in varnostne ukrepe uskladi s to uredbo v šestih mesecih od njene uveljavitve.

### 13. člen
### (prenehanje uporabe)

Z dnem uveljavitve te uredbe se preneha uporabljati Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19 in 95/21 – ZInfV-A).

### 14. člen
### (začetek veljavnosti)

Ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

Št.
Ljubljana, __. __. 2023
EVA 2022-1544-0004

Vlada Republike Slovenije
dr. Robert Golob
predsednik

**OBRAZLOŽITEV**

## I. UVOD

### 1. Pravna podlaga (besedilo, vsebina zakonske določbe, ki je podlaga za izdajo predpisa):

Zakonodaja Republike Slovenije: tretji odstavek 17. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV).

### 2. Rok za izdajo uredbe, določen z zakonom:

Rok za izdajo te uredbe je eno leto od uveljavitve Zakona o spremembah in dopolnitvi Zakona o informacijski varnosti (Uradni list RS, št. 95/21; v nadaljnjem besedilu ZInfV-A), kar je določeno v prehodni določbi drugega odstavka 12. člena (izdaja podzakonskih predpisov in strategije) ZInfV-A. Ob pregledu ureditve je bilo ugotovljeno, da so poleg spremembe oblike predpisa glede na ureditev, ki se uporablja, potrebne tudi nekatere vsebinske spremembe, kar je v danih okoliščinah izdajo te uredbe zamaknilo.

### 3. Splošna obrazložitev predloga uredbe, če je potrebna:

Po prehodni določbi 13. člena ZInfV-A je z dnem uveljavitve ZInfV-A prenehal veljati (tudi) Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. 68/19; v nadaljnjem besedilu: pravilnik), ki pa se uporablja do izdaje podzakonskih predpisov iz drugega odstavka prejšnjega člena ZInfV-A (glej tudi prehodno določbo drugega odstavka 12. člena ZInfV-A). ZInfV-A je namreč med drugim posegel tudi v tretji odstavek 17. člena osnovnega Zakona o informacijski varnosti (Uradni list RS, št. 30/18), kjer je besedilo »Minister, pristojen za informacijsko družbo (v nadaljnjem besedilu: minister)« nadomestil z besedo »Vlada«. S tem je bila z ZInfV-A spremenjena pristojnost za izdajo podzakonskega predpisa, ki ureja varnostno dokumentacijo in varnostne ukrepe organov državne uprave, pri čemer je navedena pristojnost prešla z dotlej področno pristojnega ministra (ki je izdal pravilnik) na Vlado Republike Slovenije (v nadaljnjem besedilu: vlada), ki izda uredbo. S tem v zvezi glej tudi 21. člen Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14, 55/17 in 163/22).

Predlog uredbe v največji meri ohranja dosedanjo vsebino pravilnika, ki je namenjena organom državne uprave, ki so skupina zavezancev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23; v nadaljnjem besedilu: ZInfV). Pri tem so po tretji alineji prvega odstavka 5. člena ZInfV zavezanci le tisti organi državne uprave, ki upravljajo informacijske sisteme in dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljnjem besedilu: organi državne uprave). Pri tem posamične zavezane organe državne uprave določi vlada na podlagi prvega odstavka 9. člena (določitev organov državne uprave) ZInfV. Vsebinska ureditev predlagane uredbe se glede na ureditev pravilnika spreminja in dopolnjuje le v manjšem obsegu, in sicer glede na pomanjkljivosti ureditve pravilnika, kot so bile zaznane pri njegovem izvajanju v praksi, zlasti v postopkih nadzora. Namen vsebinskih sprememb je dosedanjo ureditev dodatno izboljšati tako, da bo za uporabnike oziroma izvrševalce tega predpisa (ODU) jasnejša in lažja za uporabo ter hkrati preglednejša za potrebe poznejšega nadzora pristojnega inšpektorja. Predlogi izboljšav vsebinske ureditve v predlagani uredbi glede na pravilnik so omejeni glede na možnosti oziroma vsebino veljavnega ZInfV. Večje spremembe ureditve bodo možne šele po sprejetju novega sistemskega zakona (tako imenovani ZInfV-1), ki ga bo treba sprejeti že zaradi prenosa nove horizontalne direktive Evropske unije (EU) s področja varnosti omrežnih in informacijskih sistemov v slovenski pravni red, pri čemer gre za Direktivo (EU) 2022/2555 (direktiva NIS 2) (UL L št. 333 z dne 27. 12. 2022, str. 80), z rokom za prenos 17. 10. 2024.

Spreminja se oblika predpisa, ki je po novem uredba, ki jo izda vlada.

Z izdajo predlagane uredbe v skladu z ZInfV-A se torej upošteva načelo pravne države.

### 4. Predstavitev presoje posledic za posamezna področja, če te niso mogle biti celovito predstavljene v predlogu zakona: /

5. **Izjava o skladnosti predloga s pravnimi akti Evropske unije in korelacijska tabela, če gre za prenos direktive**

/

## II. VSEBINSKA OBRAZLOŽITEV PREDLAGANIH REŠITEV

### Obrazložitev k posameznim členom

### K 1. členu

Predlog uredbe v 1. členu določa njeno vsebino enako kot pravilnik, ki je na podlagi 13. člena ZInfV-A prenehal veljati in se še uporablja do izdaje predlagane uredbe. Pri tem se s predlagano uredbo v skladu s 17. členom ZInfV podrobneje določajo vsebina in struktura varnostne dokumentacije, metodologija za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja in pripadajočih podatkov ter minimalni obseg in vsebina varnostnih ukrepov organov državne uprave (v nadaljnjem besedilu: ODU).

### K 2. členu

Predlagana določba vsebinsko v največji meri enako kot doslej pravilnik opredeljuje pomen izrazov, uporabljenih v tej uredbi. Pri tem enako kot doslej pravilnik opredeljuje le pomen izrazov, ki niso opredeljeni z ZInfV v njegovem 4. členu.

V 2. točki predlaganega člena je bil (glede na pravilnik) dodan nov izraz »kazalnik zlorabe« (angl. *Indicator of Compromise – IOC*) zaradi rabe nove besedne zveze »kazalniki zlorabe« (angl. *Indicators of Compromise – IOCs*) v 3. točki drugega odstavka 8. člena predloga uredbe. Zato so preostale točke 2. člena glede na pravilnik preštevilčene.

Kazalnik zlorabe pomeni kazalnik, ki da informacijo o lastnostih zlorabe omrežij oziroma informacijskih sistemov ODU. Kazalnik zlorabe se uporabi za ugotavljanje možne okuženosti oziroma zlonamerne aktivnosti v teh omrežjih oziroma informacijskih sistemih.
Med kazalniki zlorabe so na primer:

- neobičajen promet, ki gre v omrežje in iz njega,
- neznane datoteke, aplikacije in procesi v sistemu,
- sumljive aktivnosti v administratorskih ali privilegiranih računih,
- neredne aktivnosti, kot je promet v državah, s katerimi ODU praviloma ne posluje,
- dvomljive prijave, dostopanje in druge omrežne dejavnosti, ki kažejo na sondiranje ali napade s surovo silo,
- zahteve in obseg branja v datotekah ODU, ki kažejo na nepravilnosti,
- omrežni promet skozi omrežna vrata, ki običajno niso uporabljena,
- velike količine stisnjenih datotek in podatkov, ki se nepojasnjeno najdejo na lokacijah, kjer ne bi smele biti.

### K 3. členu

Predlagana določba vsebinsko enako kot doslej pravilnik opredeljuje vsebino in strukturo varnostne dokumentacije, pri čemer ODU vzpostavijo in vzdržujejo dokumentirana SUVI in SUNP, ki morata zajemati najmanj elemente iz prvega odstavka 17. člena ZInfV, ter določa podpisnika te varnostne dokumentacije (predstojnik ODU). Ohranja se tudi ureditev, po kateri ODU, ki ima za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, to le vsebinsko dopolni v skladu s predlagano uredbo (prej v skladu s pravilnikom).

### K 4. členu

Predlagana določba vsebinsko v največji meri povzema pravilnik, ki opredeljuje najmanjši obseg analize obvladovanja tveganj z določitvijo sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza

obvladovanja tveganj). Pri tem se k obsegu dosedanje analize obvladovanja tveganj k dosedanjim 8 točkam uvodno dodaja nova 1. točka (druge so glede na pravilnik preštevilčene), in sicer gre pri 1. točki po novem za »navedbo uporabljene metodologije za izvedbo analize obvladovanj tveganj, ki mora biti primerljiva, verodostojna in ponovljiva«. Navedba metodologije v skladu s pravilnikom ni bila zahtevana. Ocene tveganj sicer ni mogoče narediti brez ustrezne metodologije, ki naj bi pri ODU torej obstajala. Vendar te metodologije ODU na zahtevo inšpektorja doslej ni bil zavezan predložiti. Brez poznavanja uporabljene metodologije pri ODU se zelo težko presoja analiza tveganj, ki je sicer ključna podlaga za načrtovanje in izvajanje informacijske varnosti v vsakem sistemu. Ob tem je treba pojasniti, da je uporabljana metodologija sicer lahko različna glede na področje dela ODU (različne lestvice merjenja in drugi parametri), vendar mora primerljiva, verodostojna in ponovljiva, kot je primerjalno to našteto tudi v standardu ISO 27-001. Gre torej za metodologijo, ki je primerljiva, verodostojna in ponovljiva v skladu s pravili stroke (na področju upravljanja informacijske varnosti), kot je navedeno v predlogu uredbe.

Glede na pravilnik se dopolnjuje tudi vsebina 9. točke, po kateri analiza zajema »določitev sprejemljive ravni tveganj«, in sicer tako, da je treba zdaj tudi obrazložiti določeno sprejemljivo raven tveganj (kar potrdi predstojnik ODU). Posledično bo določitev sprejemljive ravni tveganj glede na njeno obrazložitev mogoče tudi preizkusiti.

Na predlog Ministrstva za javno upravo je (glede na pravilnik) dodana še 10. točka z navedbo ukrepov za odpravo ali zmanjšanje tveganj nad sprejemljivo ravnjo. Navedeno je z vidika preventivnega delovanja ODU pri zagotavljanju informacijske in kibernetske varnosti pomembno vključiti že v fazi analize obvladovanja tveganj.

Zaradi preštevilčenja točk so bili v določbi popravljeni tudi notranji sklici.

**K 5. členu**

Predlagana določba vsebinsko v največji meri povzema pravilnik in opredeljuje najmanjši obseg politike neprekinjenega poslovanja z načrtom njegovega upravljanja, pri čemer se vsebinsko k zahtevanemu najmanjšemu obsegu (glede na pravilnik) k dosedanjim 5 točkam uvodno dodaja nova 1. točka (druge so glede na pravilnik preštevilčene). Predlagana 1. točka te določbe zahteva navedbo ciljev in načel za zagotavljanje neprekinjenega poslovanja ODU ob upoštevanju posebnosti ODU. Ker gre za politiko, ki je splošni dokument, ki ureja usmeritve, načela in cilje, ter za načrt upravljanja politike, ki je strokovni in specifični dokument, je torej potrebna ustrezna dopolnitev vsebine člena (glede na pravilnik) z novo 1. točko.

**K 6. členu**

Predlagana določba vsebinsko enako kot doslej pravilnik opredeljuje najmanjši obseg seznama ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ODU ter pripadajočih podatkov (v nadaljnjem besedilu: ključni sistemi), ki so bistvenega pomena za delovanje storitev ODU.

**K 7. členu**

Predlagana določba vsebinsko enako kot doslej pravilnik opredeljuje načrt obnovitve in ponovne vzpostavitve delovanja ključnih sistemov iz prejšnjega člena, po kateri ta zajema opis odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

**K 8. členu**

Predlagana določba v pretežni meri vsebinsko enako kot doslej pravilnik opredeljuje najmanjši obseg načrta odzivanja na incidente, ki med drugim vsebuje tudi opis protokola obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave in vsebine, ki jih mora to obvestilo zajemati.

Pri tem dodatno pojasnjujemo, da opis postopkov in odgovornosti za poročanje o incidentih zunaj ODU (po 5. točki prvega odstavka te določbe) poleg CSIRT organov državne uprave oziroma pristojnega nacionalnega organa lahko zajema tudi druge nadzorstvene organe, organe pregona in podobno (ob upoštevanju ZInfV in druge področne zakonodaje).

Obvestilo se CSIRT organov državne uprave pošlje na način, kot je objavljen na njegovi spletni strani, predviden je tudi minimalni zajem vsebine obvestila. Predvideni opis protokola obveščanja se lahko smiselno uporabi tudi za obveščanje pristojnega nacionalnega organa za informacijsko varnost, če ima ODU lastne zmogljivosti vsaj na ravni varnostno-operativnega centra.

V predlaganem drugem odstavku tega člena je (glede na pravilnik) dodana nova 3. točka (druge so bile preštevilčene), po kateri obvestilo iz 6. točke prejšnjega odstavka vsebuje tudi navedbo kazalnikov zlorabe, če le-ti seveda (pri ODU) obstajajo. Pri tem je bil zaradi rabe nove besedne zveze »kazalniki zlorabe« dodan in opredeljen nov izraz (glede na pravilnik) »kazalnik zlorabe« v 2. točki 2. člena (pomen izrazov) predloga uredbe (glej tudi obrazložitev 2. člena). Pri tem dodajamo, da bo vključitev morebitnih kazalnikov zlorabe, če ti (pri ODU) seveda obstajajo, v obvestilo nacionalnemu CSIRT olajšalo tudi reševanje incidenta, kar bi zaradi škode, ki jo lahko povzročijo incidenti, moralo biti tudi v interesu ODU.

Glede vsebinske spremembe v 7. točki (prejšnji 6. točki glede na pravilnik) drugega odstavka tega člena, ki pri zahtevi opisa vpliva incidenta na neprekinjeno izvajanje storitev ODU opušča dosedanjo vsebino pravilnika iz oklepaja »(lažji incident, težji incident, kritični incident)«, pojasnjujemo, da je bilo to besedilo opuščeno iz razloga jasnosti in skladnosti ureditve z ZInfV. Besedilo v oklepaju je namreč vzbujalo dvome pri razlagi. Po prvem odstavku 21. člena ZInfV (vrednotenje incidenta in ukrepanje) namreč priglašene incidente ob njihovem reševanju vrednotijo glede na njihovo težo (lažji incident, težji incident, kritični incident) pristojni nacionalni CSIRT (v primeru IBS) ali CSIRT organov državne uprave; če imajo organi državne uprave zagotovljene lastne zmogljivosti vsaj na ravni varnostno-operativnega centra, pa jih vrednoti pristojni nacionalni organ. Pri vrednotenju se navedeni organi lahko medsebojno posvetujejo. Vrednotenje s strani pristojnih organov (lažji incident, težji incident ali kritični incident) sicer poteka predvsem na podlagi informacij, ki jih je (v danem primeru) ODU poslal ob priglasitvi incidenta s pomembnim vplivom na neprekinjeno izvajanje storitev ODU v skladu s prvim odstavkom 18. člena ZInfV. Pri tem v skladu z ZInfV ODU pri določitvi pomembnosti vpliva incidenta upoštevajo zlasti:
– število uporabnikov, ki jih je prizadela motnja pri zagotavljanju storitve ODU,
– trajanje incidenta in
– geografsko razširjenost območja, na katero incident vpliva.
Glede na navedeno je ocena ODU o pomembnosti vpliva incidenta na neprekinjeno izvajanje storitev ODU (iz 6. točke drugega odstavka tega člena) lahko opisna, kar je bilo zaradi večje jasnosti upoštevano v predlogu uredbe.

**K 9. členu**

Predlagana določba vsebinsko enako kot doslej pravilnik ureja način izdelave načrta varnostnih ukrepov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežja in informacijskih sistemov ODU ter predpisuje lastnosti takih ukrepov.

**K 10. členu**

Predlagana določba vsebinsko v največji meri enako kot doslej pravilnik ureja način priprave metodologije za pripravo analize obvladovanja tveganj in za določitev ključnih sistemov. Pri tem v prvem odstavku predlagane določbe pri načinu priprave analize obvladovanja tveganj dodaja novo 1. točko (druge se preštevilčijo), po kateri ODU »navede metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedel analizo obvladovanja tveganj v skladu s to uredbo«. Navedba izbrane metodologije za ODU zdaj ni obvezna. Sicer analize obvladovanja tveganj ni mogoče narediti brez metodologije, ki se uporablja in naj bi pri ODU torej obstajala. Vendar te metodologije ODU na zahtevo inšpektorja doslej ni bil zavezan predložiti oziroma izkazati, katero metodologijo uporablja, če je ni sam določal. Brez poznavanja uvodno uporabljene metodologije se zelo težko presoja ustreznost celotne metodologije za analizo tveganj, ki je ključni metodološki dokument za načrtovanje in izvajanje informacijske varnosti v vsakem sistemu. Ob tem je treba pojasniti, da je uporabljana metodologija lahko različna glede na področje dela ODU, vključno glede lestvic merjenja in atributov ocenjevanja, zato je treba z vidika jasnosti, preglednosti ter preverljivosti vnaprej opredeliti tudi te.

Glede na pravilnik (tam gre za 1. točko prvega odstavka zadevnega člena) je bila vsebinsko dopolnjena tudi 2. točka prvega odstavka predlaganega člena, in sicer se izvede popis sredstev znotraj SUVI in določijo njihovi upravljavci (ter dodajajo) »oziroma odgovorne osebe za ta sredstva«, kar je potrebno zaradi jasnosti in določnosti.

Zaradi preštevilčenja točk v prvem odstavku (glede na pravilnik) je v drugem odstavku predlaganega člena popravljen tudi notranji sklic. Zadnji stavek tretjega odstavka tega člena pa je (glede na pravilnik) postal četrti odstavek.

**K 11. členu**

Predlagana določba vsebinsko v pretežni meri enako kot doslej pravilnik opredeljuje minimalni obseg in vsebino varnostnih ukrepov, ki jih na podlagi varnostne dokumentacije iz te uredbe pripravijo in izvajajo ODU. Pri tem so varnostni ukrepi organizacijski, logično-tehnični in tehnični ter zagotavljajo najmanj s to določbo predpisane vsebine.

Vsebinske spremembe so glede na pravilnik le v 3., 11. in 12. točki.

V 3. točki, ki je doslej predvidevala notranjo presojo SUVI in SUNP v rednih časovnih presledkih, se je (glede na pravilnik) beseda »presoja« nadomestila z besedo »pregled«, dodalo se je besedilo »najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov«. Besedna zveza »notranja presoja« bi glede na opozorilo Ministrstva za notranje zadeve Republike Slovenije lahko čezmerno vključevala povezavo s standardom ISO 9001 in točno določenimi oblikami ugotavljanja ustreznosti dokumentacije in postopkov, za izvedbo katerih mora oseba, ki želi izvajati notranjo presojo, imeti status notranjega presojevalca, kar pa ni namen predlagane ureditve. Ob tem smo upoštevali tudi pripombo Ministrstva za infrastrukturo Republike Slovenije, da se za naprej predvidijo enaka (najkrajša možna) obdobja rednih časovnih presledkov, in to tako, da je predvideno najkrajše obdobje rednih časovnih presledkov za notranji pregled SUVI in SUNIP enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe, ki vplivajo na zaupnost, celovitost oziroma razpoložljivost omrežij in informacijskih sistemov. Obdobje enega leta je za ODU v splošnem primerno obdobje za ponovni notranji pregled SUVI in SUNP, vendar je pri tem treba upoštevati tudi morebiti bistveno spremenjene okoliščine, ki vplivajo na informacijsko varnost ODU.

V vsebinsko novi 11. točki se predlaga nov varnostni ukrep, in sicer »upravljanje in preprečevanje izrabe tehnične ranljivosti« (omrežij in informacijskih sistemov). Predlagana dopolnitev izhaja iz v praksi ugotovljenega dejanskega stanja groženj informacijski varnosti v informacijsko-kibernetskem svetu, kjer pogosti pojavi »ranljivosti ničelnega dne« (angl. *Zero-Day Vulnerability*) pomenijo resnično veliko grožnjo.

V predlagani 12. točki je glede na pravilnik združena vsebina 11. in 12. točke, saj gre za povezan in soodvisen ukrep, ki se po tem predlogu glasi »zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop«.

**K 12. členu**

Predlagana je prehodna določba, s katero je predviden rok za uskladitev s predlogom te uredbe, ki je šest mesecev od njene uveljavitve. Predlagana uredba namreč vsebinsko uvaja tudi manjše spremembe oziroma dopolnitve glede na pravilnik, ki se še uporablja. Zato je primerno, da se ODU da ustrezen rok za uskladitev varnostne dokumentacije in varnostnih ukrepov (ki so morali biti že pripravljeni v skladu s pravilnikom) s predlagano uredbo.

Ob tem pripominjamo, da mora ODU po prehodni določbi petega odstavka 43. člena ZInfV iz leta 2018 izpolniti varnostne zahteve in zahteve za priglasitev incidentov iz 16., 17. in 18. člena tega zakona v skladu s tem zakonom v dvanajstih mesecih od njihove določitve iz prejšnjega odstavka (torej četrtega odstavka 43. člena ZInfV iz leta 2018).

**K 13. členu**

Po predlagani določbi se z dnem uveljavitve te uredbe preneha uporabljati pravilnik, ki je prenehal veljati z uveljavitvijo ZInfV-A, njegova uporaba pa je bila hkrati podaljšana do izdaje predlaganega podzakonskega predpisa (glej 13. člen ZInfV-A) – to je predlagane uredbe.

**K 14. členu**

Po predlagani določbi ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije, kar je običajen rok za uveljavitev predpisov, ki je primeren tudi za uveljavitev te uredbe.