OSNUTEK PREDLOGA **EVA 2022-1544-0003**

Na podlagi tretjega odstavka 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21) Vlada Republike Slovenije izdaja

U R E D B O

o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev

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 ter pripadajočih podatkov in minimalni obseg ter vsebino varnostnih ukrepov izvajalcev bistvenih storitev.

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. Neprekinjeno poslovanje so aktivnosti, ki so potrebne za ohranjanje poslovanja organizacije v času motenj ali prekinitev normalnega delovanja.
3. Razpoložljivost je lastnost informacij, omrežij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo.
4. Sistem upravljanja neprekinjenega poslovanja je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se na njih odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni ter vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov (v nadaljnjem besedilu: SUNP).
5. Sistem upravljanja varovanja informacij 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 (v nadaljnjem besedilu: SUVI).
6. Sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za izvajalca bistvenih storitev (v nadaljnjem besedilu: IBS) in ki zato zahteva zaščito.
7. Trajanje incidenta je časovno obdobje od prekinitve ustreznega zagotavljanja storitve v smislu razpoložljivosti, celovitosti ali zaupnosti do trenutka njene ponovne vzpostavitve.
8. Uporabnik je fizična ali pravna oseba, ki uporablja posamezno bistveno storitev neposredno, posredno ali s posredovanjem oziroma je odvisna od nje.
9. 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) IBS vzpostavijo in vzdržujejo dokumentiran SUVI in SUNP, ki mora obsegati najmanj elemente iz prvega odstavka 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21).

(2) Varnostno dokumentacijo iz prejšnjega odstavka podpiše zakoniti zastopnik IBS.

(3) Če ima IBS 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 oceno sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza obvladovanj tveganj) obsega najmanj:

1. navedbo uporabljene metodologije za izvedbo analize obvladovanj tveganj, ki mora biti primerljiva, verodostojna in ponovljiva,
2. navedbo sredstev znotraj SUVI in upravljavce teh sredstev oziroma odgovorne osebe za ta sredstva,
3. navedbo potencialnih groženj tem sredstvom,
4. navedbo ranljivosti sredstev iz 2. točke tega člena, ki bi jih lahko grožnje iz prejšnje točke prizadele,
5. navedbo vpliva uresničitve groženj iz 3. točke tega člena na razpoložljivost, celovitost in zaupnost sredstev iz 2. točke tega člena zaradi ranljivosti iz prejšnje točke,
6. oceno vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube razpoložljivosti, celovitosti ali zaupnosti,
7. realistično oceno verjetnosti, da pride do kršitve informacijske varnosti,
8. ovrednotenje ravni tveganj in
9. določitev ter obrazložitev sprejemljive ravni tveganj.

5. člen
(politika neprekinjenega poslovanja)

Politika neprekinjenega poslovanja z načrtom njegovega upravljanja (v nadaljnjem besedilu: politika neprekinjenega poslovanja) obsega najmanj:

1. navedbo ciljev in načel za zagotavljanje neprekinjenega poslovanja oziroma neprekinjenega izvajanja bistvenih storitev ob upoštevanju področnih posebnosti,
2. navedbo postopkov neprekinjenega poslovanja, ki se jo izdela 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 IBS in odpovedi storitev pogodbenih izvajalcev,
4. določitev minimalne ravni poslovanja,
5. navedbo ukrepov za zagotavljanje neprekinjenega poslovanja, ki se izdela 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 in njeno posodabljanje.

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

Seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja IBS ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev (v nadaljnjem besedilu: ključni, krmilni in nadzorni informacijski sistemi) obsega najmanj:

- navedbo sredstev znotraj SUVI, od katerih je odvisno zagotavljanje bistvenih storitev, in
- opredelitev ključnih, krmilnih in nadzornih informacijskih sistemov in navedbo njihovih upravljavcev.

7. člen
(načrt obnovitve delovanja informacijskih sistemov)

Načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnjega člena (v nadaljnjem besedilu: načrt obnovitve delovanja informacijskih 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 nacionalnega CSIRT (v nadaljnjem besedilu: načrt odzivanja na incidente) obsega 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, obravnavo in analizo incidentov informacijske varnosti, vključno z beleženjem 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 IBS in izven IBS ter
6. opis protokola obveščanja nacionalnega CSIRT o incidentu informacijske varnosti.

(2) Obvestilo iz 6. točke prejšnjega odstavka se pošlje nacionalnemu CSIRT na način, kot 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. oceno geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
4. oceno morebitnega čezmejnega vpliva incidenta,
5. oceno morebitnega medpodročnega vpliva incidenta in
6. oceno pomembnosti vpliva incidenta na neprekinjeno izvajanje bistvenih storitev (lažji incident, težji incident, kritični incident).

9. člen
(načrt varnostnih ukrepov)

(1) Pri izdelavi načrta varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov IBS upoštevajo:

- dokumente varnostne dokumentacije iz 4. do 8. člena tega pravilnika in
- posebne potrebe področja, na katerem deluje posamezen IBS.

(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 IBS usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost in se izogibajo podvajanjem,
3. skladni tako, da se primarno obravnavajo osnovne in skupne varnostne ranljivosti IBS kljub področnim posebnostim, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna področja,
4. sorazmerni s tveganji tako, da se izogiba prekomernemu bremenu za IBS,
5. konkretni tako, da IBS te varnostne ukrepe izvajajo in da ti ukrepi prispevajo h krepitvi njihove informacijske varnosti,
6. preverljivi tako, da lahko na zahtevo pristojnega organa predložijo dokazila o njihovi implementaciji,
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, KRMILNIH IN NADZORNIH INFORMACIJSKIH SISTEMOV TER PRIPADAJOČIH PODATKOV

10. člen

(metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov)

(1) IBS analizo obvladovanja tveganj pripravi tako, da:

1. določi 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 celovitosti, razpoložljivosti in zaupnosti sredstev iz prejšnje točke,
4. prepozna ranljivosti sredstev iz 2. točke tega odstavka, ki bi jih lahko grožnje iz prejšnje točke prizadele,
5. oceni stopnjo vpliva uresničitve groženj iz 3. točke tega odstavka na razpoložljivost, celovitost in zaupnost 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 oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj.

(2) IBS seznam svojih ključnih, krmilnih in nadzornih informacijskih sistemov pripravi tako, da:

- izmed popisanih sredstev znotraj SUVI iz 2. točke prejšnjega odstavka presodi, ali je zagotavljanje bistvenih storitev odvisno od posameznega sredstva znotraj SUVI, in
- izmed posameznih sredstev znotraj SUVI, od katerih je v skladu s prejšnjo točko odvisno zagotavljanje bistvenih storitev, presodi, katero izmed teh sredstev je bistveno za delovanje bistvene storitve.

(3) IBS izvede analizo obvladovanj tveganj in določi ključne, krmilne in nadzorne informacijske sisteme tako, da bodo rezultati teh postopkov dosledni, primerljivi in verodostojni.

(4) IBS izvaja analizo obvladovanj tveganj ter določa ključne, krmilne in nadzorne informacijske 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)

IBS za zagotavljanje celovitosti, zaupnosti ter razpoložljivosti omrežij in informacijskih sistemov na podlagi varnostne dokumentacije iz 3. člena tega pravilnika pripravijo in izvajajo organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki zagotavljajo najmanj:

1. podporo vodstva IBS zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja IBS,
2. integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve,
3. notranjo presojo SUVI in SUNP v rednih časovnih presledkih,
4. upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito,
5. ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja iz prejšnje točke,
6. upravljanje prometa in komunikacij,
7. opredelitev varnostnih zahtev za ključne dobavitelje IBS,
8. fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi IBS,
9. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti IBS,
10. preverjanje identitete uporabnikov,

11. upravljanje in preprečevanje izrab tehničnih ranljivosti,
12. zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop,
13. zaščito pred zlonamerno programsko kodo,
14. beleženje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev ter
15. zaznavanje poskusov vdorov in preprečevanje incidentov.

V. PREHODNA IN KONČNA DOLOČBA

12. člen
(prehodno obdobje)

(1) IBS že izdelano varnostno dokumentacijo ter varnostne ukrepe uskladi s to uredbo v šestih mesecih od njene uveljavitve.

(2) Ne glede na rok iz prejšnjega odstavka za posamezni subjekt, ki ga vlada določi za IBS na podlagi Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21) po uveljavitvi te uredbe, velja rok šest mesecev od njegove določitve za IBS za uskladitev z njo.

13. člen
(začetek veljavnosti)

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

Št.
Ljubljana, . ….2022
EVA 2022-1544-0003

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 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21; v nadaljnjem besedilu ZInfV)

2. Rok za izdajo uredbe, določen z zakonom:

Rok za izdajo te uredbe je sicer v enem letu 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 odstavku 12. člena (izdaja podzakonskih predpisov in strategije) ZInfV-A. Ob pregledu ureditve se ugotovilo, da so poleg spremembe oblike predpisa glede na ureditev, ki se uporablja, potrebne tudi še določene vsebinske spremembe, kar v danih okoliščinah izdajo te uredbe nekoliko zamika.

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 izvajalcev bistvenih storitev (Uradni list RS, št. 32/19; 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 posegi v osnovni Zakon o informacijski varnosti (Uradni list RS, št. 30/18) posegel tudi v tretji odstavek 12. člena, 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 izvajalcev bistvenih storitev, pri čemer je navedena pristojnost prešla iz dotlej resorno 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 in 55/17).

Predlog uredbe v največji meri ohranja dosedanjo vsebino Pravilnika, ki je namenjena izvajalcem bistvenih storitev in so kategorija zavezancev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21; v nadaljnjem besedilu ZInfV). Izvajalci bistvenih storitev delujejo na področjih energije, digitalne infrastrukture, oskrbe s pitno vodo in njene distribucije, zdravstva, prometa, bančništva, infrastrukture finančnega trga, preskrbe s hrano in varstva okolja (glej 5. člen ZInfV), pri čemer posamične izvajalce bistvenih storitev (javni ali zasebni subjekti) določi vlada na podlagi 6. člena 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 (IBS) 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 ureditve bi bile možne šele po spremenjeni zakonski ureditvi, kar bo v prihodnosti potrebno že zaradi nove področne direktive EU, ki naj bi bila sicer kmalu sprejeta, sledil pa bo rok (predvidoma 21 mesecev) za njen prenos v nacionalno zakonodajo

Spreminja se tudi oblika predpisa, ki je po ZInfV-A uredba, ki jo izda vlada. Z izdajo predlagane uredbe 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 UREDBE

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 z 12. členom ZInfV 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 ter pripadajočih podatkov ter minimalni obseg ter vsebino varnostnih ukrepov izvajalcev bistvenih storitev (v nadaljnjem besedilu IBS).

K 2. členu

Predlagana določba vsebinsko 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.

K 3. členu

Predlagana določba vsebinsko enako kot doslej Pravilnik opredeljuje vsebino in strukturo varnostne dokumentacije, pri čemer IBS vzpostavijo in vzdržujejo dokumentiran SUVI in SUNP, ki mora obsegati najmanj elemente iz prvega odstavka 12. člena ZInfV ter določa podpisnika te varnostne dokumentacije (zakoniti zastopnik IBS). Ohranja se tudi ureditev po kateri IBS, ki ima za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, to le vsebinsko dopolni skladno 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 oceno sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza obvladovanj tveganj). Pri tem pa se k obsegu dosedanje analize obvladovanja tveganj k dosedanjim 8. točkam uvodno dodaja novo 1. točko (ostale so glede na Pravilnik preštevilčene) in sicer gre pri 1. točki sedaj za »navedbo uporabljene metodologije za izvedbo analize obvladovanj tveganj, ki mora biti primerljiva verodostojna in ponovljiva,«. Navedba metodologije skladno s Pravilnikom ni bila zahtevana. Ocene tveganj se sicer ne da narediti brez neke metodologije, ki naj bi pri IBS torej obstajala. Vendar omenjene metodologije IBS na zahtevo inšpektorja doslej ni bil zavezan predložiti. Brez poznavanja uporabljene metodologije s strani IBS pa se zelo težko presoja analiza tveganj, ki je sicer ključni akt za načrtovanje in izvajanje informacijske varnosti v vsakem sistemu. Ob tem je treba še pojasniti, da je uporabljana metodologija sicer lahko različna glede na področje dela IBS (različne lestvice merjenja in drugi parametri), vendar mora ta metodologija biti primerljiva, verodostojna in ponovljiva, kar je upoštevano v tem predlogu. Glede na Pravilnik se dopolnjuje tudi vsebina zadnje točke, po kateri je analiza doslej obsegala »določitev sprejemljive ravni tveganj« in sicer tako, da je treba sedaj tudi obrazložitev določene sprejemljive ravni tveganj (kar potrdi najvišji organ IBS). Posledično bo določitev sprejemljive ravni tveganj glede na njeno obrazložitev, mogoče tudi preizkusiti.

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 novo 1. točko (ostale so glede na Pravilnik preštevilčene). Predlagana 1. točka te določbe zahteva navedbo ciljev in načel za zagotavljanje neprekinjenega poslovanja oziroma neprekinjenega izvajanja bistvenih storitev ob upoštevanju področnih posebnost. Ker gre za politiko, ki je splošen dokument, ki ureja usmeritve, načela in cilje ter za načrt upravljanja politike, ki je strokoven in specifičen 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 IBS ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev (v nadaljnjem besedilu: ključni, krmilni in nadzorni informacijski sistemi).

K 7. členu

Predlagana določba vsebinsko enako kot doslej Pravilnik opredeljuje načrt obnovitve in ponovne vzpostavitve delovanja informacijskih 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 vsebinsko enako kot doslej Pravilnik opredeljuje najmanjši obseg načrta odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT ter določa način obveščanja nacionalnega CSIRT ter vsebine, ki jih mora to obvestilo najmanj zajemati. Ob tem le še dodatno pojasnjujemo, da opis postopkov in odgovornosti za poročanje o incidentih izven IBS (po 5. točki prvega odstavka te določbe) poleg nacionalnega CSIRT lahko zajema npr. tudi pristojni nacionalni organ, druge nadzorstvene organe, organe pregona ipd. (ob upoštevanju ZInfV ter druge področne zakonodaje).

K 9. členu

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

K 10. členu

Predlagana določba vsebinsko v največji meri enako kot doslej Pravilnik ureja način priprave metodologije za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov. Ob tem pa v prvem odstavku predlagane določbe pri načinu priprave analize obvladovanja tveganj dodaja novo 1. točko (ostale se preštevilčijo), po kateri IBS »določi metodologijo z opredelitvijo lestvic in atributov ocenjevanja, po kateri bo izvedel analizo obvladovanja tveganj v skladu s to uredbo,«. Določitev izbrane metodologije s strani IBS sedaj ni obvezna. Sicer se analize obvladovanja tveganj ne da narediti brez uvodne določitve metodologije, ki se uporablja in naj bi pri IBS torej obstajala. Vendar omenjene metodologije IBS na zahtevo inšpektorja doslej ni bil zavezan predložiti. Brez poznavanja uporabljene metodologije se zelo težko presoja ustreznost celotne metodologije za analizo tveganj, ki je sicer ključni metodološki akt za načrtovanje in izvajanje informacijske varnosti v vsakem sistemu. Ob tem je treba še pojasniti, da je uporabljana metodologija lahko različna glede na področje dela IBS in sicer 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 določi njihove upravljavce (ter dodaja) »oziroma odgovorne osebe za ta sredstva«, kar je potrebno zaradi jasnosti in določnosti.

Zaradi preštevilčenja točk v prvem odstavku (glede na Pravilnik) je bil v drugem odstavku predlaganega člena popravljen tudi notranji sklic.

K 11. členu

Predlagana določba vsebinsko v največji meri enako kot doslej Pravilnik opredeljuje minimalni obseg in vsebino varnostnih ukrepov, ki jih na podlagi varnostne dokumentacije iz te uredbe pripravijo in izvajajo IBS. 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 točkah 11 in 12. V vsebinsko novi 11. točki se predlaga nov varnostni ukrep in sicer »upravljanje in preprečevanje izrab tehničnih 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« (Zero-Day Vulnerability) predstavljajo veliko dejansko grožnjo.
V predlagani 12. točki pa sta glede na Pravilnik združeni vsebini 11. in 12. točke Pravilnika, 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 dosedanji Pravilnik. Zato je primerno, da se IBS da ustrezen rok za uskladitev varnostne dokumentacije ter varnostnih ukrepov (ki so morali biti sicer že pripravljeni skladno s Pravilnikom) s predlagano uredbo. Če pa bo vlada po izdaji predlagane uredbe določila nove oziroma dodatne subjekte za IBS po ZInfV, se zanje predlaga rok šestih mesecev od njihove določitve za IBS za uskladitev s predlagano uredbo. Navedeno je skladno tudi s prehodno določbo drugega odstavka 43. člena osnovnega ZInfV iz leta 2018.

K 13. členu

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.