

Na podlagi 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), 3. člena Uredbe o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS št. 98/23) in 16. člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23), minister za notranje zadeve izdaja

KROVNO INFORMACIJSKO VARNOSTNO POLITIKO MINISTRSTVA ZA NOTRANJE ZADEVE

I. Vsebina, namen in cilji

1. člen (opredelitev)

- (1) Krovna informacijska varnostna politika Ministrstva za notranje zadeve Republike Slovenije (v nadaljnjem besedilu: krovna politika) skupaj s področnimi politikami informacijske varnosti (v nadaljnjem besedilu: področne politike) določa cilje in namene Ministrstva za notranje zadeve Republike Slovenije in Inšpektorata Republike Slovenije za notranje zadeve (v nadaljnjem besedilu: ministrstvo) pri ohranjanju zaupnosti, celovitosti in razpoložljivosti podatkov, informacijskih sistemov in omrežja.
- (2) Načrtovanje in uresničevanje krovne politike in področnih politik sta del procesov organiziranja in splošne strukture vodenja ministrstva, varnost pa del zasnove vseh informacijskih storitev, poslovnih procesov in organiziranja dela pri varnosti podatkov, informacijskih sistemov in omrežja.

2. člen (sestavine politik in izvedbenih dokumentov)

- (1) Krovna in področne politike sestavljajo sistem upravljanja varovanja informacij (v nadaljnjem besedilu: SUVI) in sistem upravljanja neprekinjenega poslovanja (v nadaljnjem besedilu: SUNP) v obsegu, kot ju opredeli Zakon o informacijski varnosti.
- (2) SUVI in SUNP sta znotraj ministrstva strukturirana na več ravneh. Prvo raven zastopa krovna politika, drugo raven pa področne politike, ki se nanašajo na določeno področje informacijske varnosti in neprekinjenega poslovanja.
- (3) SUVI temelji na ocenjevanju tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti v skladu z zakonodajo in mednarodnimi standardi informacijske varnosti.
- (4) SUNP temelji na pripravi načrtov za primere incidentov informacijske varnosti in motenj pri poslovanju oziroma v katastrofalnih razmerah za ministrstvo ter na ustreznem odzivu nanje, da se lahko zagotovi neprekinjeno izvajanje informacijskih storitev na sprejemljivi, vnaprej določeni ravni¹ v notranjih organizacijskih enotah (v nadaljnjem besedilu: NOE), v skladu z zakonodajo in mednarodnimi standardi neprekinjenosti poslovanja.
- (5) Dokumenti tretje ravni so navodila ter načrti o uporabi sredstev in izvajanju nalog s področja informacijske varnosti. Obrazci, ki se nanašajo na posamezno navodilo, so v prilogah teh dokumentov.
- (6) Seznam posameznih dokumentov, ki pomenijo strukturo SUVI in SUNP ministrstva, je v prilogi te

¹ Določeno v analizi vpliva na poslovanje in postopkih neprekinjenega poslovanja.

krovne politike (priloga št. 1).

3. člen (namen politik)

Namen krovne in področnih politik je vzpostaviti okvirna varnostna izhodišča za zaščito podatkov, informacijskih sistemov in omrežja, za izvajanje informacijskih storitev ter zagotavljanje delovanja poslovnih procesov ministrstva pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi.

4. člen (cilji politik)

Ministrstvo želi s politikami doseči naslednje cilje:

- zavarovati podatke, informacijske sisteme in omrežja pred nepooblaščenim dostopom,
- ohraniti celovitost podatkov, informacijskih sistemov in omrežja ter preprečiti nepooblaščen spremembe,
- zagotoviti razpoložljivost podatkov, informacijskih sistemov in omrežja, ki jih zaposleni, pogodbeni sodelavci in druge za to upravičene osebe² potrebujejo za izvajanje svojih delovnih nalog,
- ozaveščati zaposlene, pogodbene sodelavce in druge za to upravičene osebe o pomenu informacijske varnosti in neprekinjenega poslovanja ministrstva,
- vzpostaviti beleženje vseh zakonsko zahtevanih aktivnosti nad podatki, informacijskimi sistemi in omrežji,
- ustrezno obravnavati vse varnostne dogodke in incidente informacijske varnosti, ki vplivajo na podatke, informacijske sisteme in omrežja,
- raziskovati sume kršitev informacijskih varnostnih politik,
- zagotoviti skladnost ministrstva z zakoni in predpisi na področju informacijske varnosti in neprekinjenega poslovanja,
- upoštevati priporočila in dobre prakse, ki temeljijo na standardih informacijske varnosti in neprekinjenega poslovanja.

II. Pomen izrazov

5. člen (pomen izrazov)

Uporabljeni izrazi imajo za potrebe te krovne politike naslednji pomen:

- incident informacijske varnosti (v nadaljnjem besedilu: incident) je vsak dogodek, ki ima dejanski negativen učinek na varnost omrežij in informacijskih sistemov;
- informacijska varnost je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti;
- omrežje in informacijski sistem so:
 - elektronsko komunikacijsko omrežje, ki vključuje prenosne sisteme in, kjer je primerno, komutacijsko ali usmerjevalno opremo ter druge vire, vključno z omrežnimi elementi, ki niso aktivni, ki omogočajo prenos signalov po žicah, z radijskimi valovi, optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi prizemnimi omrežji, električnimi kablenskimi sistemi, če se uporabljajo za prenos signalov, omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kablenske televizije ne glede na vrsto prenesenih informacij;
 - vsaka naprava ali skupina med seboj povezanih ali sorodnih naprav, od katerih ena ali več

² drugi državni organi, študentje oziroma vse pooblaščen osebe, kjer sodelovanje ni nujno pogojeno s pogodbo

- o njih na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali
 - o digitalni podatki, ki jih elementi iz prve in prejšnje alineje te točke shranjujejo, obdelujejo, pridobivajo ali prenašajo za namene njihovega delovanja, uporabe, varovanja in vzdrževanja;
- standard je tehnična specifikacija, ki jo je sprejel priznani organ za standardizacijo, za večkratno ali stalno uporabo:
 - o ISO/IEC 27001 informacijska varnost, kibernetska varnost in varovanje zasebnosti – sistemi upravljanja informacijske varnosti – zahteve,
 - o ISO/IEC 27002 informacijska varnost, kibernetska varnost in varovanje zasebnosti – kontrole informacijske varnosti,
 - o ISO 22301 varnost in vzdržljivost – sistem vodenja neprekinjenosti poslovanja – zahteve;
- SUNP je sistem upravljanja neprekinjenega poslovanja, ki obsega dokumente, postopke in tehnične kontrole za razpoložljivost storitev in povezanih informacijskih sistemov;
- SUVI je sistem upravljanja varovanja informacij, ki obsega dokumente, postopke in tehnične kontrole varovanja informacijskih sistemov oziroma informacijske varnosti v celoti;
- politika je izraz, ki se uporablja v enakem pomenu kot v Zakonu o informacijski varnosti in drugih aktih na področju informacijske varnosti;
- tveganje je vsaka razumno določljiva okoliščina ali dogodek, ki ima lahko negativen učinek na varnost omrežij in informacijskih sistemov;
- varnost omrežij in informacijskih sistemov je zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali pripadajočih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopni;
- varnostni dogodek je vsaka zaznana kibernetska aktivnost, ki nima vpliva na omrežja, informacijske sisteme in storitve, pomeni pa dogodek, ki bi lahko ogrozil informacijsko varnost ministrstva;
- varovani podatki so podatki, pomembni za poslovanje ministrstva in delo uslužbencev.

III. Zakonske ter druge predpisane zahteve in standardi

6. člen (zakonodaja)

- (1) Ministrstvo k pripravi, vzdrževanju in izvajanju krovne in področnih politik neposredno zavezuje ta Zakon o informacijski varnosti in Uredba o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (v nadaljnjem besedilu: zakonodaja).
- (2) Ministrstvo pri pripravi krovne in področnih politik, poleg zahtev iz zakonodaje, upošteva tudi priporočila veljavnih standardov ISO/IEC 27001, ISO/IEC 27002 in ISO 22301. Izrazi, uporabljeni v krovni in področnih politikah, imajo enak pomen, kot jih določajo pojmovniki zakonodaje in pojmovniki standardov ISO/IEC 27000, ISO 22301.

7. člen (zahteve z drugih področij)

Poleg zahtev iz prejšnjega člena je ministrstvo zavezano še k izvajanju varnostnih aktivnosti, ki jih določajo:

- Zakon o tajnih podatkih (ZTP) in na njegovi podlagi sprejeta Uredba o varovanju tajnih podatkov;
- Zakon o poslovnih skrivnostih (ZPosS);
- Splošna uredba o varstvu podatkov in Zakon o varstvu osebnih podatkov (ZVOP);
- Uredba o upravnem poslovanju.

IV. Obseg in meje krovne ter področnih politik

8. člen (obseg SUVI in SUNP)

Krovna in področne politike se nanašajo na vse NOE, zaposlene, pogodbene izvajalce in druge za to upravičene osebe, podatke, informacijske sisteme, omrežja ter z njimi povezana sredstva, ki jih v okviru svojega poslovanja upravlja ministrstvo, ter postopke in ukrepe za zagotavljanje informacijske varnosti in neprekinjenega izvajanja storitev, ki jih ministrstvo zagotavlja uporabnikom.

9. člen (aktivnosti v zvezi s SUVI)

SUVI kot del sistema upravljanja na ministrstvu, katerega namen je uresničevanje krovne in področnih politik, obsega:

- ugotavljanje dogodkov znotraj in izven ministrstva, ki lahko ogrozijo celovitost in zaupnost podatkov, informacijskih sistemov in omrežij,
- oceno verjetnosti dogodkov iz prejšnje alineje,
- ukrepe za zmanjšanje verjetnosti za nastop incidenta,
- ukrepe za zmanjšanje negativnih učinkov in omilitve posledic incidenta,
- način organiziranja postopkov informacijske varnosti ministrstva, ki zagotavlja varnost podatkov, informacijskih sistemov in omrežij,
- način rednega preverjanja skladnosti izvajanih ukrepov in postopkov informacijske varnosti.

10. člen (aktivnosti v zvezi s SUNP)

SUNP obsega:

- ugotavljanje dogodkov znotraj in izven ministrstva, ki lahko ogrozijo razpoložljivost podatkov, informacijskih sistemov in omrežij;
- ugotavljanje podatkov, informacijskih sistemov in omrežij, ki vplivajo na izvajanje informacijskih storitev in poslovnih procesov;
- ugotavljanje zahtevanega časa za okrevanje informacijskih storitev in poslovnih procesov;
- določitev vpliva na poslovanje ob pojavu incidenta;
- ukrepe za zmanjšanje negativnih učinkov in omilitve posledic incidenta;
- način organiziranja neprekinjenega poslovanja ministrstva, ki zagotavlja razpoložljivost podatkov, informacijskih sistemov in omrežij,
- način rednega preverjanja skladnosti izvajanih ukrepov in postopkov.

V. Načrtovanje SUVI in SUNP

11. člen (elementi načrtovanja)

- (1) V okviru načrtovanja SUVI in SUNP ministrstvo ugotavlja tveganja in priložnosti, ki se nanašajo na:
 - možnosti, da SUVI in SUNP lahko dosežeta želene rezultate;
 - preprečitev ali zmanjšanje neželenih vplivov na informacijsko varnost in neprekinjenost poslovanja;
 - doseganje nenehnih izboljšav SUVI in SUNP.
- (2) Ministrstvo pri načrtovanju SUVI in SUNP upošteva notranje in zunanje dejavnike, ki so pomembni za njegovo delovanje in vplivajo na njegovo sposobnost doseganja želene ravni varnosti in neprekinjenega poslovanja. Pri vzpostavljanju, uvajanju in vzdrževanju SUVI in SUNP ministrstvo upošteva zlasti:

- svoje poslovne procese, informacijske storitve, NOE, zaposlene in pogodbene izvajalce, podatke, informacijske sisteme in omrežja ter z njimi povezana sredstva in potencialni vpliv morebitnih incidentov;
 - povezave med krovno in področnimi politikami ter dokumentacijo SUVI in SUNP;
 - izpostavljenost ministrstva varnostnim tveganjem in tveganjem za neprekinjeno poslovanje.
- (3) Z vidika razumevanja potreb in pričakovanj zainteresiranih strani³ ministrstvo pri vzpostavljanju svojega SUVI in SUNP opredeli:⁴
- zainteresirane strani, pomembne za SUVI oziroma SUNP ter njihove zahteve (na primer njihove potrebe in pričakovanja glede informacijske varnosti ali neprekinjenega poslovanja).
- (4) Ministrstvo vse informacije, vezane na zakonske in druge predpisane zahteve, redno dokumentira in posodablja.

VI. Ocena tveganj in analiza vpliva na poslovanje

12. člen (ocena tveganj)

Ministrstvo izdela oceno tveganj SUVI in SUNP, za katero opredeli metodologijo za izvajanje ocene tveganj, merila za izbor varnostnih ukrepov, sprejemljivo raven tveganja ter postopek obravnave preostalih tveganj. Ocena tveganj je podlaga za načrtovanje ukrepov SUVI in SUNP.

13. člen (analiza vpliva na poslovanje)

Ministrstvo izvaja analizo vpliva na poslovanje SUNP, za katero opredeli metodologijo za izvajanje analize vpliva na poslovanje, merila za izbor ukrepov in sprejemljivo raven vpliva. Analiza vpliva na poslovanje je podlaga za oceno varnostnih tveganj in ukrepov SUVI in SUNP.

VII. Podpora izvajanju krovne in področnih politik

14. člen (politika in vodenje)

Vodstvo ministrstva izkazuje zavezanost k izvajanju krovne in področnih politik s tem, da usmerja k:

- zagotavljanju, da so določene in sprejete krovna in področne politike skladne z zakonodajo na področju informacijske varnosti;
- zagotavljanju vključitev zahtev krovne in področnih politik v vse NOE;
- zagotavljanju virov, potrebnih za uvedbo in vzdrževanje krovne in področnih politik;
- učinkovitemu upravljanju SUVI in SUNP;
- nenehnemu izboljševanju SUVI in SUNP;
- podpiranju vodij NOE, da v okviru vodenja izkazujejo zavezanost k izvajanju SUVI in SUNP v skladu z njihovo odgovornostjo.

15. člen (usposobljenost in obveščenost)

Za usposobljenost in obveščenost skrbi vodja informacijske varnosti ministrstva tako, da:

³ Imetnik interesa, ki lahko vpliva na oblikovanje SUVI in SUNP. To so na primer NOE in organi ministrstva, ki zahtevajo določeno odzivnost, URSIV, ki zahteva poročanje, ali MDP in Policija, ki imata zahteve pri gostovanju v njihovem informacijskem sistemu.

⁴ Opredeljeno v opisih varnostnih zahtev procesov.

- določa zahteve glede usposobljenosti zaposlenih, pogodbenih izvajalcev in drugih za to upravičenih oseb na področju informacijske varnosti in neprekinjenega poslovanja, ki vplivajo na izvajanje njihovih delovnih nalog;
- zagotovi, da imajo zaposleni, pogodbeni izvajalci in druge za to upravičene osebe dostop do ustreznega usposabljanja;
- zaposlenim, pogodbenim sodelavcem in drugim za to upravičenim osebam zagotovi dokumentacijo SUVI in SUNP.

16. člen (ozaveščanje)

Zaposleni, pogodbeni sodelavci in druge za to upravičene osebe morajo biti seznanjene s:

- krovno politiko, področnimi politikami in dokumenti SUVI in SUNP, pomembnimi za njihovo delo;
- posledicami neskladnosti njihovega dela z zahtevami SUVI in SUNP;
- njihovo vlogo pri upravljanju z varnostnimi dogodki in incidenti.

VIII. Skrbnik krovne in področnih politik

17. člen (odgovorne osebe in NOE)

- (1) Minister imenuje vodjo informacijske varnosti ministrstva, ki je skrbnik SUVI in SUNP.
- (2) Za vodjo informacijske varnosti ministrstva izvajata podporne naloge NOE, pristojna za informacijsko varnost, ter NOE, pristojna za informatiko.
- (3) NOE, pristojna za informacijsko varnost, najmanj enkrat na leto pregleda krovno politiko, področne politike in druge dokumente SUVI in SUNP z vidika njihove skladnosti s standardi, predpisi in odločitvami ministrstva. Z ugotovitvami seznanijo vodjo informacijske varnosti ministrstva, ki ministru predlaga morebitne spremembe in dopolnitve politik.

IX. Kršitev krovne in področnih politik

18. člen (zaznavanje in obravnavanje kršitev, varnostnih dogodkov in incidentov)

- (1) Ministrstvo mora z organizacijskimi in tehničnimi ukrepi oziroma postopki zagotoviti zaznavanje kršitev krovne politike, področnih politik in dokumentov SUVI in SUNP ter njihovo sankcioniranje po področni zakonodaji ali pogodbenih določilih.
- (2) Vsi neželeni ali nepričakovani dogodki, za katere je zelo verjetno, da bodo ogrozili varnost ministrstva, morajo biti evidentirani in obravnavani kot varnostni dogodki ali incidenti.

19. člen (obveščanje)

- (1) Ministrstvo v okviru upravljanja incidentov opredeli potrebo po notranjem in zunanjem obveščanju ter določi:
 - kaj bo predmet obveščanja;
 - kdaj bo obveščanje izvedeno;
 - kdo bo obveščen.

- (2) Ministrstvo v okviru upravljanja incidentov vzpostavi, vpelje in vzdržuje navodila za:
- interno komuniciranje v zvezi z informacijsko varnostjo;
 - zunanje komuniciranje z drugimi zainteresiranimi stranmi, vključno z mediji;
 - sprejemanje, dokumentiranje in odgovarjanje na sporočila, vezana na informacijsko varnost ali neprekinjeno poslovanje;
 - prilagoditev in povezavo sistema načrtovanja v organizaciji z nacionalnim sistemom odziva na incidente (URSIV, IP-RS, SI-CERT in drugi);
 - zagotovitev opreme za komuniciranje med ključnimi zaposlenimi ob incidentih;
 - podporo strukturiranih komunikacij z drugimi organi in zagotovitev povezljivosti, kadar je to potrebno.
- (3) Zapisi o vseh incidentih, ki so vplivali na varnost ministrstva, se hranijo zakonsko predpisano časovno obdobje.

X. Varnostni forum, notranja presoja in vodstveni pregled

20. člen (varnostni forum)

Ministrstvo redno izvaja preverjanje delovanja SUVI in SUNP na varnostnem forumu, vsaj trikrat letno in po vsakem zaznanem incidentu, ki je ali bi lahko imel resen vpliv na delovanje ministrstva. Skliče ga vodja informacijske varnosti ministrstva. Sestava, vloge in postopek varnostnega foruma so določeni v Navodilu za izvajanje varnostnega foruma, notranje presoje in vodstvenega pregleda SUVI in SUNP v Ministrstvu za notranje zadeve. O varnostnem forumu mora biti izdelan zapisnik, ki ga podpiše vodja informacijske varnosti ministrstva.

21. člen (notranja presoja)

- (1) Ministrstvo najmanj enkrat letno z notranjo presojo SUVI in SUNP preveri, ali so cilji ukrepov, ukrepi, procesi in postopki, določeni v krovni in področnih politikah ter dokumentaciji SUVI in SUNP, v skladu z zakonskimi zahtevami ter ustrezno in učinkovito vpeljani ter vzdrževani.
- (2) Program notranjih presoj za obdobje treh let načrtuje vodja informacijske varnosti ministrstva, potrdi pa minister. Program notranjih presoj mora zagotoviti, da se v treh letih pregledajo vsi cilji ukrepov, ukrepi, procesi in postopki.
- (3) Za organiziranje in izvedbo notranje presoje je odgovorna NOE, pristojna za informacijsko varnost. Notranja presoja se izvede v skladu z Navodilom za izvajanje varnostnega foruma, notranje presoje in vodstvenega pregleda SUVI in SUNP v Ministrstvu za notranje zadeve. O notranji presoji mora biti izdelan zapisnik, ki ga podpiše vodja informacijske varnosti ministrstva.

22. člen (vodstveni pregled)

- (1) Minister se seznani in vsaj enkrat letno oceni izvedbo ukrepov, sprejetih na varnostnih forumih, pregleda rezultate notranjih presoj tekočega leta ter odloča o predlogih vodje informacijske varnosti ministrstva glede izboljšav oziroma sprememb na področju informacijske varnosti. V ta namen opravi vodstveni pregled, ki se zaključi z odločitvami in ukrepi za izboljšanje učinkovitosti SUVI in SUNP.
- (2) Postopek izvedbe vodstvenega pregleda je določen v Navodilu za izvajanje varnostnega foruma, notranje presoje in vodstvenega pregleda SUVI in SUNP v Ministrstvu za notranje zadeve. O vodstvenem pregledu mora biti izdelan zapisnik, ki ga podpiše minister.

XI. Objava ter dokumentiranost krovne in področnih politik

23. člen

(objava krovne politike, področnih politik ter dokumentov SUVI in SUNP)

Krovna in področne politike ter dokumenti SUVI in SUNP so objavljeni na intranetu ministrstva in dostopni vsem zaposlenim. Pogodbenim sodelavcem in drugim za to upravičenim osebam, ki imajo omogočen pooblaščen dostop do informacijskih storitev in omrežja ministrstva, mora biti še pred začetkom opravljanja nalog omogočen tudi dostop do krovne politike ter tistih področnih politik in dokumentov SUVI in SUNP, ki jih potrebujejo pri svojem delu.

XII. Končna določba

24. člen

Krovna politika začne veljati osmi dan po objavi na intranetu ministrstva. Z dnem uveljavitve te politike preneha veljati Krovna politika varovanja informacij MNZ RS, št. 024-10/2009/251 z dne 1. 2. 2011.

Številka: 007-103/2024/26

Datum: 26. 7. 2024

Boštjan Poklukar
minister

Priloga:

– št. 1 – strukturni seznam dokumentov

