

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), 16. člena Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US RS, 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) in 2. člena Krovne informacijske varnostne politike Ministrstva za notranje zadeve Republike Slovenije minister za notranje zadeve izdaja

**PODROČNO POLITIKO UPORABE INFORMACIJSKIH SISTEMOV IN OMREŽJA
MINISTRSTVA ZA NOTRANJE ZADEVE
ZA POGODBENE IZVAJALCE**

I. Namen in cilji

1. člen

Področna politika uporabe informacijskih sistemov in omrežja Ministrstva za notranje zadeve Republike Slovenije za pogodbene izvajalce (v nadaljnjem besedilu: področna politika) opredeljuje varnostna pravila za izvajanje pogodbe, ki predvideva skrbniške oziroma privilegirane dostope na informacijskih sistemih in omrežju Ministrstva za notranje zadeve Republike Slovenije in Inšpektorata Republike Slovenije za notranje zadeve (v nadaljnjem besedilu: ministrstvo). Področna politika izraža odločenost ministrstva zaščititi informacijske sisteme in omrežje, ki jih upravlja.

2. člen

Namen področne politike je postaviti izhodišča za zaščito informacijskih sistemov in omrežja pred nevarnostmi, namernimi ali naključnimi. Izvajanje področne politike je pomembno za zagotavljanje varnosti informacij oziroma podatkov in nemoteno izvajanje poslovanja ministrstva.

II. Pomen izrazov

3. člen

Uporabljeni izrazi imajo za potrebe te 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 označuje zaščito, varovanje in obrambo 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 in 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 kabelskimi sistemi, če se uporabljajo za prenos signalov, omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije ne glede na vrsto prenesenih informacij;
 - vsaka naprava ali skupina med seboj povezanih ali sorodnih naprav, od katerih ena ali več njih na podlagi programa opravlja samodejno obdelavo digitalnih podatkov, ali
 - 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.
- 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 je zapisan v Zakonu o informacijski varnosti in drugih zakonskih aktih na področju informacijske varnosti.
 - 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.
 - Varnostni incident pomeni enega ali več dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno delovanje ministrstva, povzročili poslovno škodo oziroma vplivali na zaupnost, celovitost ali razpoložljivost podatkov, aplikacij ter informacijskega sistema.
 - Varovani podatki so podatki, pomembni za poslovanje ministrstva in delo uslužbencev.

III. Področja politike

4. člen

Ministrstvo je lastnik oziroma upravljavec vseh podatkov in informacij na sredstvih informacijskega sistema, v omrežju ministrstva in v omrežju, v katerem gostuje.

5. člen

Pri pripravi tehnične dokumentacije za izvedbo javnega naročila, ki vključuje potrebo po dostopu do informacijskega sistema ali omrežja ministrstva, notranja organizacijska enota (v nadaljnjem besedilu: NOE), pristojna za informacijsko varnost, v sodelovanju z NOE, odgovorno za pripravo tehnične dokumentacije, in službo, pristojno za informatiko, izvede analizo tveganja in določi potrebne varnostne ukrepe. Dostop do informacijskega sistema ali omrežja ni dovoljen, dokler niso uveljavljeni ustrezni varnostni in nadzorni mehanizmi in ne začne veljati pogodba, ki določa pogoje dostopa.

Pravila za določanje dostopov so opredeljena v Področni politiki upravljanja informacijskih sistemov Ministrstva za notranje zadeve Republike Slovenije, ki opisuje načine dostopa in nadzor nad dostopi do informacij in informacijskega sistema ter s katero je pogodbeni izvajalec seznanjen.

Pogodbenim izvajalcem se omogoči dostop do tistih informacijskih sistemov ali omrežja, ki jih nujno potrebujejo za izvajanje pogodbe.

Pred sklenitvijo pogodbe morajo pogodbeni izvajalec, njegov podizvajalec in pri njiju zaposleni, ki bodo izvajali dela po pogodbi, podpisati izjavo o seznanitvi z varnostnimi politikami in navodili, ki so priložena k razpisni dokumentaciji, ter o njihovem sprejemanju.

6. člen

V pogodbo se vključijo najmanj določbe, ki jih za pogodbene izvajalce ministrstva določa zakonodaja s področja informacijske varnosti, in zahteve pristojnih organov za informacijsko varnost ter ustreznih varnostnih politik ministrstva.

Pogodbeni izvajalci so odgovorni za uporabo informacijskega sistema v obsegu in za namen, kot sta opredeljena s pogodbo, ter brez nepotrebnega in nedogovorjenega prekomernega obremenjevanja informacijskih sredstev.

7. člen

Pogodbeni izvajalci morajo preprečiti nepooblaščen dostop do računalniške opreme, ki jo uporabljajo za izvajanje pogodbe.

Pogodbeni izvajalci so dolžni ministrstvu sporočiti podatke o posameznikih, ki bodo opravljali dela v informacijskem sistemu ali omrežju ministrstva, za potrebe določitve skrbniškega/uporabniškega imena in dostopnih pravic ali za pregled dostopov oziroma izvajanja dela.

Pogodbeni izvajalci so odgovorni za varovanje svojih gesel in skrbniških/uporabniških imen. Gesla morajo biti varovana, uporabniška imena se ne smejo deliti z drugimi uporabniki.

Skupna skrbniška/uporabniška imena niso dovoljena. Izjemoma so dovoljena le, če je mogoče enolično določiti končnega uporabnika.

Geslo mora praviloma vsebovati najmanj 15 znakov ali več, in sicer kombinacijo malih in velikih črk, števil in posebnih znakov. Gesla, ki jih uporabljajo pogodbeni izvajalci v informacijskem sistemu ministrstva, se ne smejo uporabljati drugje. Če se gesla uporabljajo za spletne aplikacije, se vpisujejo le na varne, pravilne in zaupanja vredne povezave. V spletnih brskalnikih se ne uporablja funkcija »zapomni si geslo«. Prednostno se uporablja možnost večfaktorske avtentikacije, če je tehnično mogoča.

8. člen

Pogodbeni izvajalci ne smejo izvajati aktivnosti, ki bi lahko ogrozile varno uporabo informacijskih sistemov, kot so:

- razkritje gesla uporabniškega računa ali omogočanje uporabe lastnega skrbniškega/uporabniškega računa drugim uporabnikom,
- izvajanje vdorov v omrežne komunikacije ali motenje omrežnih komunikacij, če to ni izrecno določeno v pogodbi. Vdori poleg ostalega vključujejo dostop do podatkov, za katere posameznik nima pravice dostopa, ali prijavljanje v informacijski sistem, aplikacijo ali uporabniški račun, za katerega posameznik ni izrecno pooblaščen, ter poslušanje ali preusmerjanje komunikacijskih vrat (PORT) ali zaščit.

9. člen

Za zmanjševanje tveganj, povezanih z uporabo informacijskih sistemov in omrežij pogodbenih izvajalcev v informacijskih sistemih in omrežjih ministrstva, mora pogodbeni izvajalec poskrbeti za pravočasno nameščanje vseh varnostnih popravkov na sistemih pogodbenih izvajalcev, ki dostopajo do informacijskih sistemov ministrstva.

10. člen

Za namene upravljanja informacijske varnosti lahko vodja informacijske varnosti ministrstva kadar koli odredi nadzor nad pogodbenimi izvajalci. V primeru zaznane nesprejemljive uporabe ali ravnanja v neskladju s SUVI in SUNP lahko vodja informacijske varnosti sproži postopke upravljanja varnostnih incidentov.

IV. Varnostni incidenti

11. člen

Pogodbeni izvajalci so odgovorni za upravljanje varnostnih incidentov, groženj in ranljivosti. To vključuje takojšnjo prijavo varnostnih incidentov, kot tudi varnostnih pomanjkljivosti, nepravilnega ali sumljivega delovanja informacijskih sistemov ter nedelovanja informacijskih sistemov ministrstva na kontaktne naslove, navedene v pogodbi.

12. člen

Kjer je potrebno, se s pogodbenim izvajalcem dogovori o neprekinjenosti storitev, ki se morajo ohraniti tudi v primeru nepredvidenih dogodkov, na primer pri večjih okvarah ali nesrečah.

13. člen

Spremembe ali ugotovljene nepravilnosti v zvezi z zagotavljanjem pogodbenih storitev, ki se nanašajo na informacijsko varnost (SUVI in SUNP), se upravljajo tako, da vodja informacijske varnosti ministrstva ali NOE, pristojna za upravljanje SUVI in SUNP, o njih obvesti skrbnika pogodbe na ministrstvu. Če je v pogodbi naveden tehnični skrbnik, pa se obvesti tega. Skrbnik oziroma tehnični skrbnik na podlagi vrste sprememb ali ugotovljenih nepravilnosti:

- informira pogodbenega izvajalca o pomembnih spremembah varnostne politike;
- sodeluje pri izvajanju nadzora in spremljanju ravni izvajanja storitev in informacijske varnosti pri pogodbenem izvajalcu;
- pregleda poročila in zapise pogodbenega sodelovanja;
- spremlja spremembe pri izvajanju storitev;
- po potrebi predlaga spremembo, dopolnitev, prekinitvev ali izvedbo drugih ukrepov v zvezi s pogodbo.

V. Končna določba

14. člen

Področna politika začne veljati osmi dan po objavi na intranetu ministrstva.

Številka: 007-108/2024/19

Datum: 31.7.2024

Boštjan Poklukar
minister