Na podlagi četrtega odstavka 74.a 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 in 51/16) izdaja Vlada Republike Slovenije

U R E D B O

o informacijski varnosti

I. SPLOŠNE DOLOČBE

1. člen

(namen in področja uporabe)

(1) Ta uredba določa minimalne skupne zahteve glede informacijske varnosti, ki vključujejo enotne okvire upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi, če uredba ne določa drugače.

(2) Ta uredba velja za organe državne uprave (v nadaljnjem besedilu: organ). Uredba velja tudi za druge državne organe, organe lokalnih skupnosti, javne agencije in nosilce javnih pooblastil ter druge subjekte, ki se povezujejo s centralnim informacijsko- komunikacijskim sistemom (v nadaljnjem besedilu: povezani subjekt).

1. člen

(pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

|  |
| --- |
| 1. analiza tveganja je proces ugotavljanja narave tveganja in določitve ravni tveganja; |
| 1. analiza vpliva na poslovanje je proces ugotavljanja in ovrednotenja možnih učinkov (finančnih, na zdravje in varnost, pravnih, na ugled itd.) naravnih ali od človeka povzročenih dogodkov na poslovanje; |
| 1. avtentikacija je jamstvo, da so zatrjevane značilnosti posamezne entitete dejansko take; |
| 1. avtentikacijska sredstva so informacije, ki jih uporabnik pozna (geslo, osebna identifikacijska številka ipd.), ter oprema in naprave, ki jih uporabnik ima (varnostni žeton, magnetna kartica, RFID kartica, pametna kartica, potrdilo za elektronski podpis ipd.) za enolično predstavitev v informacijskem sistemu; |
| 1. celovitost je lastnost informacij in informacijskih sistemov, da so točne in popolne; |
| 1. dnevnik dogodkov je hramba sistemskih podatkov z zapisi vseh dogodkov v času delovanja sistema; |
| 1. dogodek informacijske varnosti je ugotovljeno stanje informacijskega sistema, storitev ali omrežja, ki kaže na možno kršitev politike informacijske varnosti ali izpad nadzorstev, ali predhodno neznane razmere, ki lahko pomembno vplivajo na varnost; |
| 1. državno komunikacijsko omrežje je omrežje, namenjeno povezovanju lokalnih omrežij organov državne uprave ter dostopu do skupnih informacijskih sistemov in storitev; |
| 1. incident informacijske varnosti je neželen dogodek informacijske varnosti ali zaporedje neželenih dogodkov informacijske varnosti, ki lahko z veliko verjetnostjo ogrozijo poslovanje in informacijsko varnost; |
| 1. informacije so obdelani, organizirani, strukturirani ali v nekem sobesedilu predstavljeni podatki; |
| 1. informacijska naprava je naprava, namenjena za zbiranje, prenos, hrambo in obdelavo podatkov; |
| 1. informacijska varnost je zagotavljanje (ohranjanje) zaupnosti, celovitosti in razpoložljivosti informacij; |
| 1. informacijski sistem so med seboj odvisni sestavni deli računalniške strojne, programske in komunikacijske opreme, ki je namenjena za obravnavo (zajemanje, procesiranje, predstavitev, hrambo, prenos ipd.) nekega informacijskega premoženja; so tudi med seboj odvisne storitve, ki zagotavljajo strežniške in omrežne vire, vire za hrambo podatkov, vire uporabniške programske opreme ipd.; |
| 1. informacijsko premoženje so podatki in informacije, ki jih je glede na poslovna in varnostna merila smiselno obravnavati kot celoto; |
| 1. izmenljivi nosilec podatkov je nosilec podatkov, ki ga je mogoče preprosto povezati z informacijsko napravo ali ločiti od nje (npr. ključ USB, polprevodniški disk, CD, DVD, trdi disk, disketa, magnetni trak ipd.); |
| 1. javni oblak je infrastruktura, ki omogoča uporabo storitev, namenjenih za odprto in splošno uporabo kogar koli; lahko je v lasti, poslovnem upravljanju ali operativnem upravljanju komercialnih, akademskih ali vladnih organizacij ali kombinaciji naštetega; nameščena je na lokaciji (lokacijah) dobavitelja storitev v oblaku; |
| 1. katastrofičen dogodek je dogodek, ki povzroči škodo velikih razsežnosti; |
| 1. kibernetski napad je napad v kibernetskem prostoru, usmerjen proti organizaciji, ki uporablja kibernetski prostor, njegov namen je motenje, onemogočanje, uničevanje ali zlonamerno nadzorovanje informacijskotehnološkega okolja ali infrastrukture ali uničevanje celovitosti podatkov ali kraja informacij; |
| 1. kibernetski prostor je globalno področje znotraj informacijskega okolja, ki ga sestavlja omrežje med seboj odvisnih infrastruktur informacijskih sistemov, vključno z internetom, telekomunikacijskimi omrežji, računalniškimi sistemi in vgrajenimi procesorji ter krmilniki; |
| 1. kriptografija je veda, ki z uporabo matematičnih metod omogoča zagotavljanje zaupnosti, celovitost ter overjanje podatkov in entitet; |
| 1. kvalificirano potrdilo za elektronski podpis je potrdilo za elektronske podpise, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uradni list EU, L 257/73); |
| 1. lastni informacijski sistem je informacijski sistem organa, za katerega pridobitev, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe ter varovanje informacijskih premoženj, ki jih ta informacijski sistem obravnava, je odgovoren ta organ; |
| 1. nadzorstvo je ukrep, ki zmanjšuje tveganje; vključuje postopke, usmeritve, naprave, prakse ali druge aktivnosti, ki zmanjšujejo tveganje; |
| 1. neprekinjenost poslovanja so aktivnosti, ki so potrebne za ohranjanje poslovanja organizacije v času motenja ali prekinitev normalnega delovanja; |
| 1. obnovitev po katastrofičnem dogodku je obnovitev delovanja informacijskega sistema in izvajanja storitev po prekinitvi delovanja zaradi katastrofičnega dogodka; |
| 1. ocenitev tveganja je celotni proces ugotavljanja tveganja, analize tveganja in ovrednotenja tveganja; |
| 1. ovrednotenje tveganja je proces primerjanja rezultatov analize tveganja z merili tveganja, da bi ugotovili, ali je tveganje oziroma njegova velikost sprejemljiva oziroma znosna; |
| 1. podatki so formalizirana predstavitev dejstev, zamisli ali navodil, primernih za človeško ali strojno komunikacijo, interpretacijo ali obdelavo; |
| 1. potrdilo za elektronski podpis je elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje najmanj ime ali psevdonim te osebe; |
| 1. prenosna informacijska naprava je prenosni računalnik, dlančnik, osebni organizator, pametni telefon ali podobna prenosna elektronska naprava, ki lahko hrani, obdeluje, prikazuje ali elektronsko prenaša podatke; |
| 1. prenosna koda je programska koda, ki se po omrežju prenaša iz oddaljenega računalniškega sistema in se izvaja na lokalnem računalniku, navadno brez uporabnikovega posredovanja; sinonim: mobilna koda; |
| 1. računalništvo v oblaku je model, ki omogoča povsod navzoč, priročen, omrežni dostop na zahtevo do skupine računalniških virov v skupni rabi (npr. omrežja, strežniki, hramba podatkov, aplikacije in storitve), ki jih je mogoče konfigurirati ter hitro zagotoviti in uporabiti ob kar najmanjšem upravljavskem naporu oziroma kar najmanjši interakciji z dobaviteljem storitev; |
| 1. razpoložljivost je lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo; |
| 1. revizijska sled je dnevnik z zapisi o operacijah nad poslovnimi podatki; |
| 1. sistem za pomoč in prijavo napak je sistem ministrstva, ki vključuje klicni center, osebje za odziv ter informacijsko infrastrukturo za upravljanje napak in incidentov; |
| 1. šifriranje je postopek, pri katerem se odkrito besedilo pretvori v zakrito z uporabo šifrirnega algoritma in šifrirnega ključa; |
| 1. škodljiva programska oprema so vsi zlonamerni programi, npr. virusi, črvi, stranska vrata, trojanski konji, vohunsko programje; |
| 1. tveganje je učinek negotovosti na zastavljene cilje; |
| 1. ugotavljanje tveganja je proces odkrivanja, prepoznavanja in opisovanja tveganj; |
| 1. uporabnik je oseba, ki uporablja računalniške ali omrežne storitve; |
| 1. varnostna kopija je po vsebini identičen prepis podatkov, izdelan zaradi njihovega zavarovanja pred izgubo, poškodovanjem ali uničenjem; |
| 1. varnostni razredi so ravni razvrščanja informacijskega premoženja in informacijskih sistemov glede na možni učinek na poslovanje organa, če bi se zgodil dogodek, ki bi ogrozil to informacijsko premoženje oziroma ta informacijski sistem; |
| 1. varnostni žeton je majhna naprava, ki jo ima imetnik pri sebi, da jo uporabi za overitev dostopa do omrežne storitve; |
| 1. zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom. |

II. UPRAVLJANJE INFORMACIJSKE VARNOSTI

1. Vloge in odgovornosti

1. člen

(odbor za upravljanje informacijske varnosti)

(1) Odbor za upravljanje informacijske varnosti (v nadaljnjem besedilu: odbor) usklajuje aktivnosti na področju informacijske varnosti v državni upravi.

(2) Člani odbora so predstavniki ministrstva, pristojnega za notranje zadeve, ministrstva, pristojnega za obrambo, ministrstva, pristojnega za zunanje zadeve, ministrstva, pristojnega za finance, ministrstva, pristojnega za javno upravo (v nadaljnjem besedilu: ministrstvo), ministrstva, pristojnega za pravosodje, Policije, Slovenske varnostno-obveščevalne agencije in Urada Vlade Republike Slovenije za varovanje tajnih podatkov. Predsednik odbora je predstavnik ministrstva.

(3) Odbor imenuje vlada. Ministrstvo zagotavlja pogoje za delo odbora.

(4) Naloge odbora so:

* obravnava programov in projektov informacijske varnosti v državni upravi,
* seznanitev z revizijskimi poročili o razmerah na področju informacijske varnosti v posameznih organih in povezanih subjektih,
* obravnava dogodkov in incidentov informacijske varnosti, ki vplivajo ali bi lahko vplivali na več organov in
* poročanje o razmerah na področju informacijske varnosti vladi.

(5) Odbor uredi način svojega dela s poslovnikom, h kateremu da soglasje vlada.

1. člen

(naloge ministrstva)

(1) Ministrstvo izvaja na področju informacijske varnosti naloge, ki vključujejo:

* izvajanje varnostnih pregledov in preizkusov informacijskih sistemov,
* odobravanje uporabe storitev v javnem računalniškem oblaku,
* zagotavljanje varnega izbrisa ali uničenja nosilcev podatkov,
* odzivanje na incidente informacijske varnosti v državni upravi,
* opravljanje dinamičnih analiz tveganja in incidentov informacijske varnosti ter spremljanje razmer,
* zagotavljanje usposabljanja in ozaveščanja na področju informacijske varnosti,
* odobravanje oddaljenega dostopa do državnega komunikacijskega omrežja uporabnikom informacijskih naprav,
* upravljanje sistema za pomoč in prijavo napak,
* spremljanje incidentov v organih in povezanih subjektih,
* zagotavljanje zgodnjega opozarjanja, obveščanja in razširjanja informacij o tveganjih in incidentih informacijske varnosti organom in povezanim subjektom ter
* izmenjevanje informacij o incidentih informacijske varnosti s skupinami za odzivanje na incidente informacijske varnosti v državi in tujini.

(2) Določbe prve do šeste alineje prejšnjega odstavka ne veljajo za informacijske sisteme za področje obrambe, varstva pred naravnimi in drugimi nesrečami, policije, obveščevalno-varnostne dejavnosti, zunanjih zadev, preprečevanja in odkrivanja pranja denarja in financiranja terorizma ter opravljanja plačilnega prometa za proračunske uporabnike.

1. člen

(odgovorne osebe organa in povezanega subjekta)

(1) Za informacijsko varnost znotraj organa je odgovoren predstojnik tega organa.

(2) Za izvajanje posameznih ključnih nalog na področju informacijske varnosti znotraj organa predstojnik organa določi osebo, zadolženo za upravljanje sistema informacijske varnosti (v nadaljnjem besedilu: vodja informacijske varnosti).

(3) Če ima organ lastne informacijske sisteme, predstojnik poleg vodje informacijske varnosti določi še:

* osebe, odgovorne za pridobitev, razvoj, integracijo, spreminjanje, delovanje, vzdrževanje, varovanje in prenehanje uporabe posameznih informacijskih sistemov in za njihovo varovanje ter varovanje informacijskih premoženj, ki jih ti informacijski sistemi obravnavajo (v nadaljnjem besedilu: skrbnik informacijskega sistema), in
* osebe, organizacijske enote ali organizacije, ki skrbijo za učinkovito nameščanje, konfiguriranje, integracijo, vzdrževanje, delovanje ter izvajajo druge naloge operativnega upravljanja in varovanje posameznih informacijskih sistemov v skladu z navodili skrbnikov teh informacijskih sistemov, sprejetimi notranjimi akti organa, operativnimi navodili in sprejetimi standardi na področju informacijske varnosti (v nadaljnjem besedilu: upravljavec informacijskega sistema).

(4) Predstojnik povezanega subjekta določi osebo, zadolženo za vprašanja informacijske varnosti (v nadaljnjem besedilu: koordinator informacijske varnosti), ki predstavlja kontaktno točko za vprašanja informacijske varnosti v povezanem subjektu.

(5) Organi in povezani subjekti posredujejo imena in kontaktne podatke vodij in koordinatorjev informacijske varnosti ministrstvu.

1. člen

(vodja informacijske varnosti)

Vodja informacijske varnosti v posameznem organu je zadolžen za:

* obravnavo dogodkov in incidentov informacijske varnosti,
* pripravo in vzdrževanje operativnih navodil informacijske varnosti organa,
* preverjanje skladnosti delovanja organa s to uredbo ter operativnimi navodili informacijske varnosti organa,
* upravljanje ukrepov in postopkov varovanja informacij v informacijskih sistemih organa ter nadzor nad njimi,
* sodelovanje pri usklajevanju poslovnih in varnostnih ciljev organa,
* izvedbo ocenitve tveganj informacijske varnosti organa in upravljanje teh tveganj ter
* redno poročanje predstojniku.

1. člen

(skrbnik informacijskega sistema)

Skrbnik informacijskega sistema, ki je praviloma poslovni uporabnik tega sistema, je zadolžen, da:

* informacijski sistem in informacijsko premoženje, ki ga ta informacijski sistem obravnava, uvršča v varnostne razrede z vidika zaupnosti, celovitosti in razpoložljivosti,
* določa stopnjo zaščite informacijskega sistema,
* odloča o spremembah in dopolnitvah informacijskega sistema,
* odloča, kdo in kako sme uporabljati storitve in informacije informacijskega sistema,
* odloča o uvedbi, upravljanju in vzdrževanju priporočenih varnostnih nadzorstev ter
* odobri prenos programske oziroma strojne opreme v obratovalno okolje.

1. člen

(upravljavec informacijskega sistema)

Upravljavec informacijskega sistema je zadolžen za:

* uvedbo varnostnih nadzorstev v informacijski sistem, ki ga upravlja, in njihovo upravljanje v skladu z navodili skrbnika tega informacijskega sistema,
* spremljanje informacijske varnosti v posameznih informacijskih sistemih in odzivanje na dogodke in incidente informacijske varnosti,
* poročanje o dogodkih in incidentih informacijske varnosti v skladu z določbami o upravljanju incidentov informacijske varnosti v tej uredbi in
* sodelovanje v programih usposabljanja in ozaveščanja na področju informacijske varnosti.

2. Tveganja informacijske varnosti

1. člen

(ocenitev tveganj informacijske varnosti)

(1) Organ na podlagi ocenitve tveganj informacijske varnosti uvede ustrezne ukrepe za preprečitev ali omilitev neželenih učinkov in zagotovi nenehno izboljševanje.

(2) Organ izvaja ocenitve tveganj informacijske varnosti najmanj enkrat letno in kadar so predlagane ali nastanejo bistvene spremembe v informacijskih sistemih in delovnih procesih, pri čemer upošteva merila za sprejem tveganj in merila za izvajanje ocenitve tveganj informacijske varnosti.

(3) Organ hrani dokumentirane informacije o ugotovitvah ocenitev tveganj in obravnave tveganj informacijske varnosti.

(4) Ocenitev tveganja se izvaja v skladu z enotno metodologijo upravljanja tveganj informacijske varnosti v državni upravi, ki se objavi na spletni strani ministrstva.

(5) Na podlagi ugotovitev ocenitve tveganja organ vzpostavi nova ali prilagodi obstoječa upravljavska, operativna in tehnična nadzorstva.

3. Popis in razvrščanje informacijskega premoženja in informacijskih sistemov

1. člen

(popis informacijskega premoženja in informacijskih sistemov)

(1) Organ prepozna in popiše svoje informacijsko premoženje in informacijske sisteme.

(2) Popis informacijskega premoženja in informacijskih sistemov mora biti natančen, ažuren in usklajen z drugimi popisi.

(3) Vsakemu informacijskemu premoženju in informacijskemu sistemu se dodeli skrbnik.

(4) Popis informacijskega premoženja in informacijskih sistemov se izvaja v skladu z enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi, ki se objavi na spletni strani ministrstva.

1. člen

(razvrščanje, označevanje in zaščita informacijskega premoženja in informacijskih sistemov)

(1) Organ zagotovi, da je njegovo informacijsko premoženje ustrezno zaščiteno v skladu z njegovim pomenom zanj, zato se informacijsko premoženje razvrsti v varnostne razrede glede na vrednost, pomembnost in občutljivost za nepooblaščeno razkritje, spreminjanje ali razpoložljivost.

(2) Informacijske sisteme se razvrsti v varnostne razrede v skladu z razvrstitvijo informacijskih premoženj, ki jih ti sistemi hranijo, obdelujejo ali drugače obravnavajo oziroma ščitijo.

(3) Razvrstitvena shema s poimenovanjem varnostnih razredov, merila za uvrščanje informacijskega premoženja in sistemov v posamezni varnostni razred ter postopki razvrščanja in označevanja so v prilogi, ki je sestavni del te uredbe.

4. Ozaveščanje in usposabljanje

1. člen

(programi ozaveščanja in usposabljanja)

(1) Organi in povezani subjekti zagotavljajo, da se vsi njihovi uslužbenci vključujejo v programe ozaveščanja in usposabljanja s področja informacijske varnosti.

(2) V programih ozaveščanja in usposabljanja se uslužbenci organa in povezanih subjektov:

* seznanijo s svojimi vlogami in odgovornostmi na področju informacijske varnosti,
* seznanijo z varnostnimi zahtevami in
* naučijo izvajati svoje varnostne naloge.

(3) Uslužbenci organa in povezanih subjektov, ki opravljajo naloge razvoja in upravljanja informacijskih sistemov, se poleg splošnih usposabljanj s področja informacijske varnosti usposabljajo tudi na specifičnih področjih informacijske varnosti glede na naloge, ki jih opravljajo.

(4) Gradivo za osnovno usposabljanje in ozaveščanje na področju informacijske varnosti pripravlja in vzdržuje ministrstvo ter je na voljo za uporabo na ministrstvu in na spletni strani ministrstva.

5. Dokumentacija informacijske varnosti

1. člen

(obvezni dokumenti)

Organ, ki ima lastne informacijske sisteme, pripravi in sprejme naslednja dokumenta informacijske varnosti o upravljanju in izvajanju postopkov informacijske varnosti v organu:

* operativna navodila in
* načrt neprekinjenosti poslovanja in obnovitve informacijskih sistemov po katastrofičnem dogodku.

1. člen

(operativna navodila)

(1) Za zagotovitev pravilnega in varnega izvajanja nalog upravljavcev in uporabnikov informacijskega sistema se za vsak informacijski sistem izdelajo operativna navodila.

(2) V operativnih navodilih za uporabo informacijskega sistema se opišejo postopki za namestitev in konfiguracijo informacijskega sistema, zagon in zaustavitev informacijskega sistema, varnostno kopiranje, obnovo informacijskega sistema, upravljanje napak, upravljanje revizijske sledi in informacij sistemskega beleženja, vzdrževanje programske in strojne opreme, ravnanje z izmenljivimi nosilci podatkov, upravljanje računalniškega okolja in izvajanje drugih nadzorstev, ki zagotavljajo zanesljivo in varno delovanje informacijskega sistema.

(2) Operativna navodila se izdela pred prenosom informacijskega sistema v obratovalno okolje in se jih da na voljo vsem uporabnikom, ki jih potrebujejo.

1. člen

(načrt neprekinjenosti poslovanja in obnovitve informacijskih sistemov po katastrofičnem dogodku)

(1) Organ izdela, redno preverja in vzdržuje načrt neprekinjenosti poslovanja. Načrt neprekinjenosti poslovanja je zbirka postopkov in informacij, ki so pripravljene in vzdrževane tako, da se lahko uporabijo v primeru katastrofičnega dogodka. Načrt vsebuje najmanj:

* opis vlog in odgovornosti uslužbencev organa v postopkih zagotavljanja neprekinjenosti poslovanja,
* seznam ključnih poslovnih in podpornih funkcij in procesov,
* oceno tveganja,
* opis ukrepov za zagotavljanje neprekinjenosti poslovanja,
* opis postopkov odziva v sili in logistike ter
* opis postopkov obnovitve po katastrofičnem dogodku.

(2) Načrt neprekinjenosti poslovanja se preverja ob vsaki večji spremembi poslovanja in informacijskih sistemov oziroma najmanj enkrat letno ter se po potrebi dopolnjuje.

(3) Upravljavci informacijskega sistema skupaj s skrbnikom in uporabniki informacijskega sistema redno izvajajo simulacije izpadov informacijskega sistema, njegovih delov ali posameznih delovnih postaj ter preverjajo zmožnost obnovitve.

(4) O preverjanju načrta neprekinjenosti poslovanja se vodijo zapisi. O izsledkih se redno poroča predstojniku organa.

1. člen

(specifične potrebe informacijske varnosti)

Zaradi specifičnih potreb informacijske varnosti lahko organ sprejme akt, s katerim določi prilagoditve varnostnih zahtev po tej uredbi tem specifičnim potrebam.

6. Upravljanje incidentov informacijske varnosti

1. člen

(postopki upravljanja incidentov informacijske varnosti)

Organ in povezani subjekt vzpostavita mehanizme za:

* spremljanje, zaznavanje, analiziranje in poročanje o dogodkih in incidentih informacijske varnosti,
* beleženje aktivnosti upravljanja incidentov in
* odziv na incidente, vključno s postopki za stopnjevanje ukrepov informacijske varnosti, postopki za nadzorovano obnovo po incidentu in komunikacijo z notranjimi ali zunanjimi osebami ali organizacijami.

1. člen

(zaznava dogodkov in incidentov informacijske varnosti)

(1) Organ in povezani subjekt vzpostavita postopke za zaznavo dogodkov in incidentov informacijske varnosti v informacijskem sistemu in delovnem okolju.

(2) Kjer je mogoče in smiselno, se uvedejo samodejni sistemi za zaznavo, beleženje in analizo dogodkov in incidentov informacijske varnosti.

1. člen

(obveščanje in poročanje o dogodkih informacijske varnosti)

(1) Uslužbenec organa oziroma povezanega subjekta nemudoma obvesti vodjo informacijske varnosti oziroma koordinatorja informacijske varnosti o dogodku informacijske varnosti, če zazna:

* neučinkovit nadzor nad varnostjo v informacijskih sistemih,
* odstopanja od pričakovane celovitosti, zaupnosti ali dostopnosti informacij,
* človeške napake,
* neskladnost s politikami ali navodili,
* kršitev ureditve fizične varnosti, ki bi lahko vplivala na informacijsko varnost,
* nenadzorovane sistemske spremembe,
* motnje v delovanju programske ali strojne opreme,
* kršitve dostopa ali
* druge sumljive okoliščine.

(2) Pogodbene izvajalce se zaveže k obveščanju iz prejšnjega odstavka s pogodbo.

(3) Vodja informacijske varnosti oziroma koordinator informacijske varnosti beleži informacije o dogodkih informacijske varnosti v organu oziroma povezanem subjektu.

(4) Če vodja informacijske varnosti oziroma koordinator informacijske varnosti presodi, da gre za tak dogodek informacijske varnosti, ki vpliva ali bi lahko vplival tudi na druge organe ali druge povezane subjekte ali bi za njegovo obravnavo potreboval zunanjo pomoč, o tem dogodku poroča ministrstvu prek sistema za pomoč in prijavo napak.

(5) Poročilo o dogodku informacijske varnosti vsebuje naslednje informacije:

* identifikacijsko oznako dogodka,
* podatke o osebi, ki poroča,
* opis dogodka, ki vsebuje podatke o tem, kaj, kako in zakaj se je zgodil, katero premoženje je bilo prizadeto, kakšni so bili negativni poslovni učinki ter katere so zaznane ranljivosti, in
* podrobnosti o dogodku, ki vključujejo podatke o tem, kdaj se je zgodil, kdaj je bil odkrit, kdaj se je poročalo o njem, ali je zaključen in koliko časa je trajal.

(6) Ministrstvo o dogodku informacijske varnosti lahko zbere dodatne informacije in presodi, ali gre za incident informacijske varnosti.

1. člen

(poročanje o incidentih informacijske varnosti)

(1) Če gre za incident informacijske varnosti, ministrstvo pripravi poročilo o incidentu informacijske varnosti, ki poleg podatkov iz prejšnjega člena vsebuje še podatke o:

vrsti incidenta informacijske varnosti, glede na grožnjo (naravna ali druga nesreča, javni nemiri, fizična poškodba, odpoved infrastrukture, učinki sevanja, tehnična okvara, škodljivo programje, tehnični napad, kršitev pravil, ogrožanje funkcij, ogrožanje informacij, škodljiva vsebina, drugo),

prizadetih sestavnih delih oziroma sredstvih,

negativnih poslovnih učinkih (nepooblaščeno razkritje informacij, nepooblaščena sprememba, nerazpoložljivost, uničenje, drugo),

stroških obnove po incidentu,

reševanju incidenta,

povzročiteljih incidenta in njihovih nagibih,

izvedenih aktivnostih za odpravo posledic incidenta,

nadaljnjih aktivnostih,

končni oceni incidenta in

subjektih, obveščenih o incidentu.

(2) Obveščanje in poročanje o incidentih informacijske varnosti se izvaja v skladu z navodili, ki se objavijo na spletni strani ministrstva.

1. člen

(odziv na incidente in upravljanje incidentov informacijske varnosti)

(1) Na incidente informacijske varnosti se odziva: najprej vodja informacijske varnosti organa oziroma koordinator informacijske varnosti, če ta odziv ni zadosten, ministrstvo, in če je potrebno, tudi drugi organi, pristojni za obravnavo incidentov.

(2) Odziv vključuje:

omejitev škode in zagotovitev zahtevane ravni informacijske varnosti,

zbiranje in zavarovanje dokazov čim prej po incidentu,

odpravo posledic incidenta, ki lahko vključuje obnovo podatkov, informacijskih sistemov in poslovanja,

zagotavljanje, da se vse odzivne aktivnosti ustrezno beležijo za poznejšo analizo,

sporočanje obstoja incidenta informacijske varnosti ali kakršnih koli pomembnih podrobnosti o njem drugim notranjim ali zunanjim osebam ali organizacijam, ki morajo biti obveščene,

proučitev pomanjkljivosti informacijske varnosti, ki so povzročile incident ali prispevale k njegovemu nastanku, in zmanjšanje ali odpravo tveganj, ki so bila povezana z incidentom, ter

zaključevanje in arhiviranje incidenta, ko je bil uspešno razrešen.

7. Upravljanje sprememb in varnostna presoja informacijskih sistemov

1. člen

(upravljanje sprememb)

(1) Pred uvedbo spremembe informacijskega sistema se o njej obvesti vse subjekte, na katere bo sprememba predvidoma vplivala.

(2) Informacijska varnost je sestavni del upravljanja sprememb.

(3) Spremembe v informacijskem sistemu, ki vplivajo na funkcionalnost ali varnost, se izvede le na podlagi pisnega soglasja skrbnika informacijskega sistema. Spremembe se dokumentira.

(4) V procesu upravljanja sprememb se oceni varnostne vplive spremembe in preveri varnostna ustreznost spremenjenega informacijskega sistema in ustreznost varnostnih nadzorstev.

(5) O pogojih za izvedbo sprememb v obratovalnem okolju se dogovorita skrbnik informacijskega sistema in upravljavec informacijskega sistema. Spremembe, ki zahtevajo prekinitev delovanja informacijskega sistema, je treba načrtovati in vnaprej napovedati.

(6) Ob izvajanju sprememb informacijskega sistema je treba zagotoviti tako raven zaupnosti, celovitosti in razpoložljivosti informacijskega sistema, ki je skladna z njegovim varnostnim razredom.

(7) Pred vsako spremembo informacijskega sistema se izdela načrt povrnitve v prejšnje stanje.

1. člen

(varnostna presoja informacijskih sistemov)

(1) Skrbnik informacijskega sistema zagotovi izvedbo varnostne presoje informacijskega sistema v fazah zasnove, razvoja, uvedbe in obratovanja ter ob spremembi informacijskega sistema, ki ima oziroma bi lahko imela vpliv na varnost v informacijskem sistemu obravnavanega informacijskega premoženja.

(2) V postopku varnostne presoje se najmanj:

* pregleda sistemska arhitektura, da se preveri, ali temelji na dobrih varnostnih načelih in izpolnjuje varnostne zahteve,
* pregledajo ocena tveganja in varnostne zahteve informacijskega sistema, da se preveri, ali je zagotovljena ustrezna zaščita informacijskega premoženja, ki ga informacijski sistem obdeluje, hrani ali prenaša,
* pregleda preostala dokumentacija informacijskega sistema (operativna navodila, postopki v sili in načrt varnostnega kopiranja in obnovitve po katastrofičnem dogodku), da se preveri, ali je celovita in ustreza okolju, v katerem obratuje informacijski sistem, ter
* oceni uvedba nadzorstev, da se preveri, ali so bila nadzorstva uvedena in ali delujejo učinkovito.

(3) Postopek varnostne presoje se dokumentira.

(4) Varnostno presojo informacijskega sistema izvede od razvijalca tega sistema neodvisen presojevalec.

8. Odnosi z dobavitelji blaga in storitev

1. člen

(informacijska varnost v odnosih z dobavitelji)

(1) Organ vzpostavi in izvaja nadzorstva za upravljanje dostopa dobaviteljev do informacijskih sistemov in informacij organa v skladu z določbami te uredbe.

(2) Dobavitelje se s pogodbo zaveže, da bodo smiselno upoštevali vse določbe iz poglavja Temeljna nadzorstva za zagotavljanje informacijske varnosti te uredbe.

1. člen

(informacijska varnost v pogodbah z dobavitelji)

V pogodbe z dobavitelji se vključijo določbe, ki urejajo specifične zahteve za zagotavljanje informacijske varnosti in se nanašajo na:

* opis informacij, do katerih se dostopa, in načine dostopa do njih,
* zahteve zakonodaje in predpisov, vključno z zaščito podatkov, pravicami intelektualne lastnine in avtorskimi pravicami, ter opis, kako se bo zagotovilo, da bodo izpolnjene,
* obvezo vsake pogodbene stranke za uvajanje in izvajanje dogovorjenih nadzorstev,
* pravila dovoljene rabe informacijskih sistemov in informacij,
* izrecni seznam osebja dobavitelja, ki ima dostop do informacijskih sistemov in informacij organa, ter opis postopkov za odobritev in preklic odobritve za dostop osebja dobavitelja do informacijskih sistemov in informacij organa,
* postopke in zahteve za upravljanje incidentov v skladu z določbami te uredbe,
* kontaktno osebo dobavitelja in organa za vprašanja informacijske varnosti,
* zahteve glede varnostnega preverjanja, če je zakonsko predpisano, za osebje dobavitelja,
* pravico do presoje postopkov dobaviteljev in uporabljenih nadzorstev ter
* odgovornost dobavitelja, da upošteva varnostne zahteve organa.

1. člen

(postopki dobave izdelkov in storitev informacijske in komunikacijske tehnologije)

Postopki dobave izdelkov in storitev informacijske in komunikacijske tehnologije se določijo v pogodbah. Določbe pogodb se nanašajo na:

* informacijskovarnostne zahteve za dobavo informacijskega in komunikacijskega tehnološkega izdelka ali storitve,
* zahteve, da dobavitelji informacijskih in komunikacijskih tehnoloških storitev upoštevajo varnostne zahteve organa glede ustrezne varnostne prakse v celotni dobavni verigi,
* proces nadzora in potrjevanja, da so izdelki in storitve informacijske in komunikacijske tehnologije skladni z navedenimi varnostnimi zahtevami,
* zagotovila, da dostavljeni izdelki informacijske in komunikacijske tehnologije delujejo, kot je pričakovano, brez nepričakovanih ali neželenih funkcij in
* postopke za upravljanje življenjskega cikla in dostopnosti sestavnih delov informacijske in komunikacijske tehnologije ter povezanih varnostnih tveganj.

1. člen

(nadzor nad storitvami dobaviteljev)

Organ izvaja nadzor nad storitvami dobaviteljev, s čimer zagotovi izvajanje z informacijsko varnostjo povezanih pogodbenih določb. Organ v okviru nadzora:

* spremlja ravni učinkovitosti storitev,
* pregleduje poročila dobaviteljev o storitvah in sklicuje redne sestanke o napredku,
* izvaja presoje dobaviteljev v zvezi s pregledi poročil neodvisnih presojevalcev, če so na voljo, in ukrepa glede težav, ki jih prepozna,
* zagotavlja informacije o incidentih informacijske varnosti ter pregled teh informacij v skladu s pogodbenimi določili in določili te uredbe,
* pregleduje revizijske sledi dobaviteljev in zapise o dogodkih informacijske varnosti, operativnih težavah, odpovedih, sledenju okvar in prekinitev, povezanih z izvedenimi storitvami,
* rešuje in obvladuje morebitne prepoznane težave,
* pregleduje informacijske varnostne vidike dobaviteljevega odnosa s svojimi dobavitelji,
* zagotavlja, da ima dobavitelj dovolj zmogljivosti za izvajanje storitev in izvedljive načrte, ki zagotavljajo ohranjanje dogovorjenih ravni neprekinjenosti storitev po večjih incidentih ali nesrečah, in
* skrbi za stalno možnost vpogleda v varnostne aktivnosti, kot so: upravljanje sprememb, prepoznavanje ranljivosti in poročanje o njih ter odzivanje na incidente informacijske varnosti z jasno opredeljenimi procesi poročanja.

1. člen

(spremembe storitev dobaviteljev)

Če se storitve dobaviteljev spremenijo, organ zagotovi, da se obstoječi informacijski varnostni postopki in nadzorstva ohranijo ali izboljšajo, skladno s pomembnostjo poslovnih informacij, sistemov in vključenih procesov, oceno tveganj in določbami te uredbe.

III. TEMELJNA NADZORSTVA ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

1. Varnostno kopiranje

1. člen

(načrtovanje in izvajanje varnostnega kopiranja)

(1) Načrt varnostnega kopiranja je del načrtovanja neprekinjenosti poslovanja. Načrt varnostnega kopiranja zagotavlja, da ne pride do izgube informacij, ki so pomembne za poslovanje organa in uporabnike storitev organa.

(2) Varnostne kopije podatkov v informacijskem sistemu se izdelujejo, hranijo in preverjajo v skladu z oceno tveganja, varnostnim razredom informacijskega premoženja in zahtevami skrbnika informacijskega sistema. Zahteve za izdelavo varnostnih kopij določajo, katere podatke naj vsebuje varnostna kopija, kako pogosto naj se izdelujejo varnostne kopije ter kje in kako dolgo se hranijo. Postopek izdelave varnostnih kopij, hranjenja in njihove ponovne uporabe se dokumentira.

(3) Samodejne postopke izdelave in obnove varnostnih kopij se redno preverja, da se zagotovi celovitost podatkov, ki se hranijo.

(4) Zahtevana nadzorstva za hrambo varnostnih kopij podatkov so enaka kot za izvirno zbirko podatkov.

(5) Pred prenosom informacijskega sistema v obratovalno okolje se pripravijo navodila za izdelavo, hrambo in preverjanje varnostnih kopij podatkov, ki jih ta informacijski sistem obravnava. Ta navodila so sestavni del operativnih navodil in se redno posodabljajo.

2. Fizična in okoljska varnost

1. člen

(varnost okolja)

Prostore, kjer so nameščene za delovanje organa oziroma povezanega subjekta ključne informacijske naprave (strežniki, pomnilniške naprave, telefonske centrale, omrežna vozlišča in drugo), se ustrezno zaščiti pred fizičnim vdorom, krajo, požarom, vdorom vode, izpadi električnega omrežja, onesnaženjem, temperaturnimi nihanji, elektromagnetnimi vplivi in drugimi okoljskimi grožnjami v skladu z veljavnimi predpisi, standardi, navodili proizvajalcev informacijske opreme in oceno tveganja.

1. člen

(fizični dostop)

(1) Vzpostavijo se nadzorstva, ki preprečujejo fizični dostop nepooblaščenih oseb do informacijskih sistemov in informacijskih premoženj.

(2) Nepooblaščene osebe v območja, kjer je možnost dostopa do informacijskih sistemov oziroma informacij, ki niso javno dostopne, dostopajo le v spremstvu pooblaščene osebe. Vsak dostop se evidentira.

1. člen

(varovanje sredstev za dostop)

(1) Vsak posameznik, ki prejme sredstva za dostop do varovanih območij in prostorov, ta sredstva varno in skrbno hrani, skladno z navodili, ki jih izda organ oziroma povezani subjekt. Sredstva se vrnejo, ko prenehajo razlogi, zaradi katerih so bila dodeljena.

(2) Sredstva za dostop niso prenosljiva na tretjo osebo.

1. člen

(kraja, izguba, zloraba ali sum zlorabe sredstva za dostop)

(1) Kraja, izguba, zloraba ali sum zlorabe sredstva za dostop se obravnava kot incident informacijske varnosti, ki se zabeleži in o njem poroča v skladu z določbami o dogodkih in incidentih informacijske varnosti iz te uredbe.

(2) Kraja, izguba, zloraba ali sum zlorabe sredstva za dostop se nemudoma prijavi tudi izdajatelju tega sredstva, ki temu sredstvu onemogoči nadaljnje dostope.

1. člen

(namestitev informacijskih naprav)

(1) Vse informacijske naprave se namesti in zaščiti tako, da je tveganje zaradi okoljskih nevarnosti in nepooblaščenega dostopa kar najmanjše.

(2) Informacijske naprave nameščajo le za to usposobljene in pooblaščene osebe v skladu z veljavnimi predpisi, standardi in pogodbenimi določili.

(3) Prosti priključki komunikacijske opreme v prostorih ne smejo omogočati nepooblaščenega dostopa do omrežja.

1. člen

(varovanje zaupnosti podatkov)

(1) Uslužbenci organa oziroma povezanega subjekta ne smejo puščati nosilcev s podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, na odprtih površinah pisarniške opreme ali drugih mestih, kjer so dostopni nepooblaščenim osebam.

(2) Izven delovnega časa organa oziroma povezanega subjekta in kadar uslužbenci organa oziroma povezanega subjekta niso fizično prisotni v prostoru, se vsa pisarniška oprema, kjer se hranijo podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, zaklene ali drugače zavaruje, informacijske naprave pa fizično ali programsko zaklenejo oziroma zavarujejo.

(3) V času, ko uslužbenec organa oziroma povezanega subjekta ni prisoten, mora biti zaslon informacijske naprave, ki se nahaja v pisarniškem okolju, zaklenjen ali naprava odjavljena.

3. Primerna uporaba informacijskih naprav in storitev

1. člen

(uporaba informacijskih naprav organa)

(1) Informacijske naprave organa so namenjene za službeno uporabo. Izjemoma se lahko uporabljajo za zasebne namene, vendar taka uporaba ne sme povzročiti dodatnih stroškov, ovirati uporabe za službene namene in ogrožati informacijske varnosti.

(2) Predstojnik organa lahko določi omejitve uporabe informacijskih naprav iz prejšnjega odstavka.

(3) Uslužbenec organa z informacijskimi napravami organa ravna kot dober gospodar, skladno s priporočili proizvajalca in upravljavca informacijskega sistema. Posege vanje opravljajo samo pooblaščene osebe.

(4) Pred prenehanjem delovnega razmerja mora uslužbenec organa odstraniti vse podatke zasebne narave in zasebno korespondenco z informacijskih naprav organa, ki so mu bile dodeljene v uporabo. Organ uslužbencu omogoči, da si zasebne podatke in zasebno korespondenco pred odstranitvijo kopira na lastne nosilce podatkov. O brisanju in kopiranju se izdela in podpiše zapisnik.

1. člen

(uporaba zasebnih informacijskih naprav)

(1) Zasebnih informacijskih naprav ni dovoljeno povezovati v informacijske sisteme državne uprave. Z njimi ni dovoljeno prenašati podatkov organa ali jih hraniti na njih.

(2) Ne glede na določbo prejšnjega odstavka se zasebne informacijske naprave, ki ustrezajo tehnološkim standardom in zmogljivostim informacijskih sistemov državne uprave, s katerimi se povezujejo, in ne zahtevajo dodatnih ali posebnih virov za namestitev in upravljanje, lahko izjemoma uporabljajo tudi za službene namene, če so upoštevane operativne zahteve za zagotavljanje informacijske varnosti iz te uredbe in uporaba take informacijske naprave ne povečuje tveganja informacijske varnosti.

(3) Povezovanje in uporabo zasebnih informacijskih naprav zagotovi upravljavec informacijskega sistema, s katerim se zasebne naprave povezujejo, na podlagi pisne odobritve skrbnika tega informacijskega sistema.

(4) Upravljavec lokalnega omrežja zagotovi mehanizme za odkrivanje nedovoljenih naprav v omrežju. Če se zazna nedovoljena naprava, se naprava odstrani ali onemogoči, zadeva pa se obravnava kot varnostni incident v skladu z določbami o dogodkih in incidentih informacijske varnosti iz te uredbe.

1. člen

(prenos informacijskega premoženja v drug informacijski sistem)

(1) Prenos informacijskega premoženja v drug informacijski sistem ali napravo je dovoljen le ob pisnem soglasju skrbnika izvornega informacijskega sistema in pod pogojem, da je v sprejemnem informacijskem sistemu ali napravi zagotovljena najmanj enaka raven varovanja zaupnosti in celovitosti teh podatkov oziroma informacij, kot v izvornem informacijskem sistemu.

(2) Raven varovanja zaupnosti in celovitosti prenesenega informacijskega premoženja v sprejemnem informacijskem sistemu in morebitno uvedbo dodatnih varnostnih ukrepov določi skrbnik izvornega informacijskega sistema, skrbnik sprejemnega informacijskega sistema pa mora tako raven varovanja zagotoviti.

1. člen

(uporaba sistema elektronske pošte)

(1) Sistem elektronske pošte organa je namenjen za službeno uporabo. Uporaba za druge namene je dopustna le izjemoma, če ne ogroža varnosti informacijskega sistema organa, ne ovira službene uporabe sistema elektronske pošte in ne zmanjšuje učinkovitosti dela drugih uslužbencev organa.

(2) Uslužbenci organa uporabljajo sistem elektronske pošte tako, da pri tretjih osebah, ki so prejemniki elektronskih sporočil, ne nastane dvom, ali gre za službeno sporočilo ali zasebno sporočilo, ki je samo poslano s službenega elektronskega naslova.

(3) Za zagotovitev varnosti in nemotenega delovanja upravljavec sistema elektronske pošte ali predstojnik organa na podlagi ocene tveganja lahko omeji:

* največjo velikost elektronskih sporočil pri pošiljanju ali sprejemanju elektronskih sporočil skupaj s priponko,
* pošiljanje nekaterih vrst priponk, med katerimi so vse izvršljive datoteke in datoteke, ki jih ni mogoče preveriti s sistemi za odkrivanje škodljive programske kode,
* vsebino s seznama prepovedanih vsebin in
* spreminjanje nastavitev predala elektronske pošte.

(4) Seznam nedovoljenih datotek iz druge alineje prejšnjega odstavka in seznam prepovedanih vsebin iz tretje alineje prejšnjega odstavka vzdržuje upravljavec sistema elektronske pošte.

(5) Elektronske pošte ni dovoljeno samodejno preusmerjati na druge naslove.

(6) Podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z2, se lahko pošiljajo po elektronski pošti le v šifrirani obliki, podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z3, pa le v šifrirani obliki na način, ki ga je odobril organ za kriptografsko zaščito podatkov.

(7) Vsa elektronska sporočila, ki se ne potrebujejo več za službene namene, je treba redno brisati iz poštnega predala. Pri shranjevanju elektronskih sporočil je treba upoštevati načela varnosti in gospodarnosti, izogibati se je treba hranjenju dokumentov v formatih, ki zavzemajo veliko količino prostora.

1. člen

(uporaba interneta)

(1) Uslužbenci organa uporabljajo internet za službene namene. Uslužbenci organa lahko internet izjemoma uporabljajo tudi za zasebne namene, vendar ta uporaba ne sme povzročati tveganj informacijske varnosti in je dovoljena samo v zmernem obsegu, ki ne ovira ali ogroža normalnega delovnega procesa.

(2) Uporaba interneta vsebinsko ni omejena. Na podlagi ocene tveganja in drugih okoliščin lahko skrbnik državnega komunikacijskega omrežja ali predstojnik organa omeji dostop do spletnih mest in storitev:

* ki lahko vsebujejo škodljivo programsko kodo ali kako drugače ogrožajo informacijska premoženja in sisteme državne uprave,
* ki lahko negativno vplivajo na razpoložljivost in odzivnost informacijskih in komunikacijskih sistemov,
* ki kršijo avtorske pravice,
* katerih vsebina lahko neposredno ali posredno ogrozi državno varnost in državljane,
* katerih vsebina bi bila lahko žaljiva za posamezne osebe ali skupine,
* če bi tak dostop lahko škodil ugledu organa in
* če bi tak dostop lahko povzročil odškodninsko odgovornost organa.

1. člen

(uporaba storitev v javnem oblaku)

(1) Storitve računalništva v javnem oblaku se lahko uporabljajo le za obravnavo informacijskih premoženj, ki niso uvrščena v varnostne razrede ali so uvrščena v varnostne razrede Z1, C1 in R1.

(2) Uporabo storitev računalništva v javnem oblaku za službene potrebe pisno odobri ministrstvo. Ministrstvo preveri, ali so varnost, zasebnost in druge upravljavske informacijsko-tehnološke zahteve ponudnika storitev računalništva v javnem oblaku ustrezno obravnavane, ob upoštevanju namena uporabe in vrste podatkov.

(3) Za vse storitve v javnem oblaku, pri katerih mora uporabnik soglašati s pogoji uporabe, besedilo soglasja pregleda in odobri ministrstvo.

(4) Uporaba storitev mora biti v skladu z določbami te uredbe o sprejemljivi uporabi, uporabi interneta in uporabi lastnih naprav na delovnem mestu.

(5) Uporaba storitev mora biti v skladu z obstoječimi predpisi, ki se nanašajo na osebne podatke, dokumentarno in arhivsko gradivo, finančne podatke podjetij ali katere koli druge podatke, ki so v lasti državne uprave ali se zbirajo v njej.

(6) Zasebnih računov za storitve v javnem oblaku ni dovoljeno uporabljati za hrambo, obdelavo ali izmenjavo podatkov organa.

4. Škodljiva programska oprema in prenosna koda

1. člen

(zaščita pred škodljivo programsko opremo)

(1) Snemanje, nameščanje in uporaba neodobrene programske opreme niso dovoljeni. Uporabniku se nameščanje programske opreme na delovno postajo onemogoči.

(2) Na strežnikih, delovnih postajah in prenosnih informacijskih napravah se namesti in redno posodablja programska oprema za zaznavo in odpravo škodljive programske opreme, ki je namenjena za pregledovanje informacijskih naprav in podatkovnih medijev in zagotavlja:

* preverjanje datotek na magnetnih ali optičnih medijih in datotek, prejetih prek omrežij, preden se uporabijo, glede okuženosti s škodljivo programsko opremo,
* preverjanje priponk elektronske pošte in snetih datotek, preden se uporabijo, na poštnih strežnikih, namiznih računalnikih, ob vstopu v omrežja itd. in
* preverjanje spletnih strani, glede vsebovanja škodljive programske opreme.

(3) Zaznana škodljiva programska oprema se prepozna, osami in odstrani.

1. člen

(ukrepanje ob okužbi s škodljivo programsko opremo)

(1) V primeru okužbe ali suma okužbe s škodljivo programsko opremo uporabnik takoj preneha uporabljati prizadete informacijske naprave in poroča o dogodku v skladu z določbami o upravljanju incidentov informacijske varnosti iz te uredbe.

(2) Škodljivo programsko opremo odstrani za to usposobljeni upravljavec informacijskega sistema.

1. člen

(nadzor nad prenosno kodo)

Uporaba prenosne (mobilne) kode se nadzoruje in se dopusti le, če so ocenjena tveganja sprejemljiva. Izvajanje neodobrene prenosne kode se, kjer je to mogoče, prepreči z ustreznimi ukrepi. Ukrepi za zaščito pred izvajanjem neodobrenih aktivnosti prenosne kode so:

* preverjanje izvajanja prenosne kode v logično osamljenem okolju,
* blokiranje kakršne koli uporabe prenosne kode,
* blokiranje sprejema prenosne kode,
* aktiviranje tehničnih ukrepov, ki so razpoložljivi v posameznih sistemih, za obvladovanje prenosne kode,
* nadzor nad razpoložljivimi viri za dostop do prenosne kode in
* kriptografska nadzorstva za zanesljivo avtentikacijo prenosne kode.

5. Varnost nosilcev podatkov

1. člen

(upravljanje izmenljivih nosilcev podatkov)

(1) Nosilci podatkov neznanega ali sumljivega izvora se ne smejo uporabljati in se predajo vodji informacijske varnosti, ki zagotovi preveritev izvora in morebitne okuženosti z zlonamerno programsko kodo.

(2) Izguba ali kraja izmenljivih nosilcev podatkov se takoj prijavi v skladu z določbami o dogodkih in incidentih informacijske varnosti iz te uredbe.

(3) Hrambo podatkov informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, na izmenljivih nosilcih podatkov, pisno odobri skrbnik informacijskega sistema, v katerem se ti podatki izvorno obravnavajo. Podatke informacijskega premoženja, ki je uvrščeno v varnostni razred Z2, se zavaruje s šifriranjem z uporabo primernih postopkov za šifriranje, podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z3, pa s postopki za šifriranje, ki jih odobri organ, pristojen za kriptografsko zaščito podatkov.

1. člen

(varen izbris in uničenje podatkov)

(1) Uporabnik in skrbnik informacijskega sistema zagotovita, da so nosilci podatkov, ki se ne potrebujejo več in vsebujejo podatke informacijskega premoženja, ki je uvrščeno v varnostni razred Z1, Z2 ali Z3, uničeni ali da so podatki varno izbrisani tako, da ni mogoče njihovo prepoznavanje oziroma njihova obnovitev.

(2) Organi, ki ne morejo sami zagotoviti varnega izbrisa ali uničenja nosilcev podatkov, jih predajo v uničenje ministrstvu.

6. Varnost programske opreme

1. člen

(razvoj in pridobitev programske opreme)

(1) Informacijska varnost se upošteva v vseh fazah razvojnega cikla programske opreme in je sestavni del vseh projektov njenega razvoja in uvedbe.

(2) Funkcionalne, tehnične in jamstvene varnostne zahteve se določijo in uvedejo kot del sistemskih zahtev.

(3) Zagotovita se testno in razvojno okolje, ki sta ločena od obratovalnega okolja.

(4) Razvijalci programske opreme uporabljajo pri pisanju kode varne programerske prakse, ki vključujejo:

* zasnovo programske opreme, ki omogoča uporabo najnižje možne ravni pravic, potrebnih za izvedbo naloge,
* preprečitev privzetega dostopa,
* preverjanje povratnih vrednosti za vse sistemske klice in
* preverjanje veljavnosti vseh vnosov.

(5) Vsi pridobljeni in razviti sistemi se ustrezno dokumentirajo.

(6) Izvorno kodo in dokumentacijo aplikativne programske opreme, razvite po meri, je treba varno hraniti in mora biti dostopna.

(7) Če se programska oprema razvije ali pridobi pri zunanjem razvijalcu oziroma dobavitelju, se določbe tega člena smiselno vključijo v pogodbo z zunanjim razvijalcem oziroma dobaviteljem.

1. člen

(prenos v obratovalno okolje)

(1) Pred prenosom nove programske opreme, njene nove različice ali popravka v obratovalno okolje se opravijo in dokumentirajo vsi predhodni razvojni in preizkusni postopki. Dokumentacija vsebuje poročila o uporabniških in zmogljivostnih preizkusih, varnostni presoji in preizkusih skladnosti ter dokazila o izpolnjevanju naročnikovih zahtev.

(2) Programska oprema mora izpolnjevati vse pravne zahteve glede avtorskih in sorodnih pravic.

1. člen

(nameščanje programske opreme)

(1) Nameščanje in spreminjanje sistemske in aplikativne programske opreme izvaja upravljavec informacijskega sistema v soglasju s skrbnikom informacijskega sistema.

(2) Skrbnik posameznega informacijskega sistema za vso programsko opremo zagotovi, da bodo določeni:

* pravice brisanja, kopiranja in spreminjanja programske opreme,
* mesto hrambe kopij programske opreme,
* osebe, odgovorne za ažurnost kopij in
* način hrambe licenčne dokumentacije.

1. člen

(standardizirano obratovalno okolje)

(1) Delovne postaje uporabljajo standardizirano obratovalno okolje. V standardiziranem obratovalnem okolju se:

* odstrani nepotrebno programsko opremo in nepotrebne uporabniške račune,
* onemogoči ali odstrani nepotrebne funkcije ali storitve,
* vzpostavi dostopna nadzorstva na objektih s ciljem, da se sistemskim uporabnikom in programom omeji dostop na najmanjši obseg, potreben za izvedbo njihovih nalog, in
* namesti nadzorstva, ki omejujejo vstopne in izstopne omrežne povezave.

(2) Možne ranljivosti v standardiziranih obratovalnih okoljih in sistemih se zmanjšajo tako, da se:

* preimenuje privzete račune,
* zamenja privzeta gesla,
* odstrani nepotrebna skupna raba datotek,
* zagotovi ažurnost popravkov,
* onemogoči dostop do nepotrebnih vhodnih in izhodnih funkcionalnosti ter
* odstrani račune, ki se ne uporabljajo.

(3) Pri spletnih, poštnih, datotečnih in drugih strežnikih z velikim tveganjem, ki so povezani z nenadzorovanimi omrežji, se:

* vzdržuje učinkovito funkcionalno ločevanje med strežniki, ki zagotavlja neodvisno obratovanje,
* ustrezno omeji komunikacija med strežniki na najmanjšo mero tako na omrežni kot na datotečni ravni in
* omeji dostop uporabnikom z upravljavskimi pravicami in programom za upravljanje informacijskega sistema na najmanjšo mero, potrebno za izvedbo njihovih nalog oziroma funkcij.

(4) Preveri se celovitost vseh strežnikov, katerih funkcije so ključne za organ, in tistih, ki so prepoznani kot strežniki z velikim tveganjem. Informacije o celovitosti strežnika se varno hrani zunaj strežnika tako, da je zagotovljena njihova neoporečnost. Informacije o celovitosti strežnika se posodablja po vsaki odobreni spremembi sistema.

(5) Za ugotavljanje ogrožanja celovitosti ali nepravilno izvedene sistemske spremembe se redno primerja shranjene informacije o celovitosti z obstoječimi informacijami na strežniku. Vse zaznane spremembe se rešujejo kot incidenti informacijske varnosti v skladu z določbami o dogodkih in incidentih informacijske varnosti po tej uredbi.

7. Nadzor nad dostopom

1. člen

(dostopne pravice)

(1) Dostop do informacij, storitev in upravljanja informacijskih sistemov je mogoč na podlagi dostopnih pravic. Te dodeljuje, spreminja in ukinja skrbnik informacijskega sistema ali upravljavec informacijskega sistema na podlagi pisne zahteve skrbnika informacijskega sistema.

(2) Dostopne pravice se dodelijo tako, da omogočajo uporabniku dostop do najmanjšega možnega nabora storitev, funkcij in informacij, ki so potrebne za opravljanje njegovih nalog.

(3) Loči se uporabniške in upravljavske dostopne pravice.

(4) Pravice do dostopa do informacijskega sistema, informacij in storitev se redno preverja in posodablja. Dostopne pravice se nemudoma spremeni ali ukine, če uporabnik zamenja delovno mesto, prekine delovno ali pogodbeno razmerje ali če se spremeni ali preneha potreba po dostopu.

(5) Dostopne pravice uporabnikov se dokumentira. Razvidi vsebujejo informacije o identiteti uporabnika, o ravni oziroma vrsti dostopnih pravic in o tem, kdaj je bil dostop odobren, kdaj so bile dostopne pravice spremenjene in kdaj so bile dostopne pravice odvzete.

1. člen

**(postopki avtentikacije)**

Informacijski sistemi morajo uporabljati najmanj enega od naslednjih postopkov avtentikacije uporabnikov:

* avtentikacijo, temelječo na geslu, pri kateri informacijski sistemi zagotavljajo uporabo gesel, ki so v skladu z zahtevami iz 54. člena te uredbe,
* avtentikacijo, temelječo na infrastrukturi javnih ključev, pri kateri informacijski sistem preveri veljavnost certifikata s preverjanjem certifikacijske poti in informacije o statusu certifikata, zagotovi pooblaščen dostop do odgovarjajočega zasebnega ključa in poveže avtenticirano identiteto z imetnikom računa,
* osebno registracijo ali registracijo prek zaupanja vredne tretje stranke, pri kateri se zahteva, da poteka registracijski postopek za prejem avtentikacije osebno ali prek zaupanja vredne tretje stranke pred registracijskim organom s pooblastilom pristojne osebe organa,
* avtentikacijo, temelječo na varnostnem žetonu, kjer se zagotovi, da informacijski sistemi uporabljajo mehanizme, ki izpolnjujejo zahteve glede kakovosti varnostnih žetonov, ki jih predpiše organ, pristojen za kriptografsko zaščito podatkov.

1. člen

(večfaktorska avtentikacija)

(1) Informacijski sistemi zagotovijo prepoznavanje in potrjevanje pristnosti uporabnikov in procesov, ki delujejo v imenu uporabnika, z večfaktorsko avtentikacijo:

* za oddaljeni dostop in
* za lokalni dostop, če informacijski sistemi obravnavajo podatke informacijskega premoženja, ki je uvrščeno v varnostne razrede Z3 ali C3.

(2) Za oddaljeni dostop informacijski sistemi, ki obravnavajo podatke informacijskega premoženja, ki je uvrščeno v varnostne razrede Z3 ali C3, uporabljajo mehanizme, ki omejujejo število ponovitev poskusov dostopa.

(3) Za oddaljeni dostop informacijski sistemi, ki obravnavajo podatke informacijskega premoženja, ki je uvrščeno v varnostne razrede Z3 ali C3, uporabljajo večfaktorsko avtentikacijo tako, da je eden od faktorjev zagotovljen z napravo, ki je ločena od sistema, do katerega se dostopa, in ta naprava izpolnjuje zahteve, ki jih predpiše organ, pristojen za kriptografsko zaščito podatkov.

1. člen

(varnost gesel)

(1) Sistemi za preverjanje ustreznosti gesel ne smejo dovoljevati gesel, ki so krajša od osmih znakov. Za vpis gesla morajo omogočiti dolžino najmanj 64 znakov. Dovoljevati morajo vse znake, ki jih je mogoče izpisati, in presledek.

(2) Sistemi za preverjanje ustreznosti gesel ne smejo dovoljevati uporabe gesel, ki:

* so na seznamu neprimernih gesel,
* so besede iz slovarja,
* vsebujejo ponavljajoče znake ali znake v zaporedju ali
* vsebujejo besede, ki jih je mogoče povezati z uporabo ali uporabnikom, kot npr. ime storitve, uporabniško ime ali izpeljanke iz njih.

(3) Uporabniki ne smejo uporabljati istih gesel za službeno in zasebno uporabo.

(4) Gesla, ki so bila ali se zanje sumi, da so bila razkrita ali ukradena, je treba nemudoma spremeniti. Če bi dolgotrajnejša pogosta uporaba istega gesla povečevala tveganje za njegovo razkritje ali krajo, je treba geslo občasno spreminjati.

(5) Vsa gesla uporabniških računov so osebna in se ne smejo deliti z drugimi osebami.

(6) Vsa gesla se obravnavajo kot podatki informacijskega premoženja, ki je uvrščeno v varnostni razred Z3. Nešifrirana gesla razen začasnih se ne smejo vključiti v sporočilo e-pošte ali sporočila drugih sporočilnih sistemov. Gesla razen začasnih se ne smejo razkriti po telefonu. Gesla se ne smejo zapisovati in hraniti na prosto dostopnih mestih v pisarni. Gesla se ne smejo hraniti v datoteki na računalniškem sistemu ali prenosni napravi v nešifrirani obliki. Začasna gesla, ki se dodelijo uporabniku, mora uporabnik spremeniti v najkrajšem možnem času.

(7) Aplikacije morajo zagotoviti avtentikacijo vsakega posameznega uporabnika in ne skupin. Aplikacije ne smejo hraniti gesel v nešifrirani obliki ali obliki, ki bi bila preprosto povračljiva. Aplikacije ne smejo pošiljati gesel prek omrežja v nešifrirani obliki.

1. člen

(nadzor nad dostopom do državnega komunikacijskega omrežja)

(1) Vstopne točke v državno komunikacijsko omrežje so pod nadzorom skrbnika državnega komunikacijskega omrežja, ki s politiko upravljanja omrežja določa načine povezav, protokole, storitve, mehanizme varovanja in nadzora nad omrežjem ter dovoljeno uporabo.

(2) Overjanje uporabnikov za dostop do državnega komunikacijskega omrežja in dostop sta izvedena z avtentikacijskim sredstvom, ki ga določi skrbnik omrežja.

(3) Do državnega komunikacijskega omrežja imajo dostop uslužbenci organa in povezanega subjekta ter tisti pogodbeni izvajalci, ki imajo pravno podlago za uporabo storitev v omrežju organa in so pridobili soglasje skrbnika informacijskega sistema, do katerega potrebujejo dostop.

(4) Uporabnik prejme avtentikacijsko sredstvo in namensko programsko opremo po tem, ko skrbnik državnega komunikacijskega omrežja odobri dostop.

(5) Za zagotavljanje zaupnosti mora biti ves podatkovni promet od končne točke zunanjega omrežja do državnega komunikacijskega omrežja šifriran.

(6) Povezovanje informacijskih sistemov je dovoljeno le po nadzorovanih in varovanih vstopno-izstopnih točkah, skozi katere potekajo storitve.

8. Spremljanje varnosti in dnevniško beleženje dogodkov

1. člen

(spremljanje varnosti)

(1) Informacijski sistemi imajo vzpostavljen sistem nadzora nad delovanjem, ki vključuje postopke obveščanja o težavah v delovanju in izpadih sistema ter postopke obveščanja o odpravi težav. Sistem nadzora nad delovanjem se uskladi z oceno tveganja, ki je izdelana za informacijski sistem.

(2) Upravljavci informacijskega sistema se na dogajanja v informacijskem sistemu dosledno odzivajo s ciljem zagotavljanja učinkovitega in varnega delovanja informacijskega sistema.

1. člen

(dnevniki dogodkov)

(1) Zapisi o uporabi in delovanju informacijskih sistemov se sprotno beležijo v dnevnike dogodkov.

(2) Zagotovi se celovitost dnevnikov dogodkov.

(3) Dnevniki dogodkov morajo omogočiti prepoznavo procesov in oseb, ki so uporabljale informacijske sisteme, pregledovale podatke, jih spreminjale ali brisale.

(4) Dnevniki dogodkov se uporabljajo za ugotavljanje ranljivosti, napak in ustreznosti nadzorstev ter za reševanje incidentov in ugotavljanje zlorab.

(5) Če dnevnik dogodkov vsebuje informacije, ki so uporabne za preiskavo varnostnega incidenta ali za preverjanje uporabe in delovanja informacijskega sistema, ali informacije v zvezi s tekočo transakcijo, ali informacije, ki bi jih bilo mogoče uporabiti kot dokaz v disciplinskih ali kazenskih postopkih, se ta dnevnik ohrani.

(6) Čas hrambe dnevnikov dogodkov se določi na podlagi zakonskih zahtev in pomembnosti informacij, ki jih hranijo, za zagotavljanje pravilnega in varnega delovanja informacijskih sistemov ter za zagotavljanje dokazov v morebitnih disciplinskih in kazenskih postopkih.

(7) Dnevniki dogodkov, ki vsebujejo osebne podatke, se hranijo največ 90 dni. Daljše obdobje hrambe je dopustno ob pisni analizi tveganja in pisni utemeljitvi potrebe po daljši hrambi, ki jo potrdi predstojnik organa oziroma povezanega subjekta. Po preteku obdobja hrambe se ti dnevniki dogodkov nepovratno izbrišejo.

(8) Določbe prejšnjega odstavka ne veljajo za dnevnike dogodkov, ki zagotavljajo sledljivost obdelave osebnih podatkov, in katerih rok hrambe izhaja iz zakona, ki ureja varstvo osebnih podatkov, ter za dnevnike dogodkov, ki zagotavljajo sledljivost sprememb arhivskega gradiva, in katerih rok hrambe izhaja iz predpisov, ki urejajo arhivsko gradivo.

1. člen

(ravnanje na podlagi ugotovitev iz dnevnikov dogodkov)

Na podlagi sporočil posameznih informacijskih sistemov ali posameznih mrežnih naprav se obravnavajo tisti dnevniški zapisi, ki nakazujejo napako na napravi ali nedovoljeno dejavnost. Upravljavec informacijskega sistema take zapise obravnava kot incident informacijske varnosti, ukrepa skladno s svojimi pristojnostmi in zagotovi ustrezno obveščanje.

9. Kriptografija

1. člen

(primerne kriptografske rešitve)

Uporabljajo se tisti kriptografski algoritmi, programska in strojna kriptografska oprema ter sistemi za upravljanje ključev, ki jih odobri organ, pristojen za kriptografsko zaščito podatkov, in tisti, ki ustrezajo varnostnim zahtevam, temelječim na oceni tveganja.

1. člen

(uporaba šifriranja)

(1) Uporaba šifriranja je obvezna pri povezovanju informacijskih sistemov, ki obravnavajo podatke informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, če se povezujejo prek nezavarovanega območja.

(2) Šifriranje podatkov se uporablja na vseh komunikacijskih povezavah, ki povezujejo geografsko ločene lokacije, med katerimi podatkovni promet poteka po nezavarovanem območju.

(3) Informacijsko premoženje, ki je uvrščeno v varnostni razred Z2 ali Z3 in se nahaja zunaj varovanih območij, se šifrira tudi v času hrambe, ne glede na format hrambe ali tip nosilca podatkov, če uredba ne določa drugače.

1. člen

(potrdila za elektronski podpis)

Pri poslovanju v državni upravi se lahko uporabljajo:

* kvalificirana potrdila za elektronski podpis,
* potrdila za elektronski podpis, določena z zakonom ali drugim predpisom, in
* potrdila za elektronski podpis, ki jih odobri minister, pristojen za javno upravo.

10. Varnost prenosnih informacijskih naprav in dela na terenu

1. člen

(prenosne informacijske naprave)

(1) Uporabnike prenosnih informacijskih naprav se seznani z dodatnimi tveganji, ki so jim izpostavljene prenosne informacijske naprave, kadar jih odnesejo iz varovanega pisarniškega okolja.

(2) Uporabniki so odgovorni za redno zaščitno kopiranje podatkov, ki so shranjeni na prenosnih informacijskih napravah.

(3) V primeru izgube, poškodbe, okvare ali kraje prenosne informacijske naprave uporabnik o tem nemudoma obvesti organizacijsko enoto ali osebo, pristojno za fizično varnost, in o incidentu poroča v skladu z določbami te uredbe o upravljanju incidentov informacijske varnosti.

(4) Hrambo podatkov informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, na prenosnih informacijskih napravah pisno odobri skrbnik informacijskega sistema, v katerem se ti podatki izvorno obravnavajo. Te podatke se ustrezno zavaruje s šifriranjem.

(5) Oddaljen dostop do državnega komunikacijskega omrežja uporabnikom prenosnih informacijskih naprav odobri in omogoči ministrstvo, če za to obstaja poslovna potreba. Uporabnik sme uporabljati le varni odobreni način povezave v državno komunikacijsko omrežje iz nevarovanih omrežij, temelječ na mehanizmih navideznega zasebnega omrežja, ki vključuje zanesljive postopke identifikacije in avtentikacije.

(6) Za vse prenosne informacijske naprave se vzpostavi postopek za uničenje, zaklepanje in oddaljeno brisanje podatkov.

1. člen

(delo na terenu)

(1) Prenosne informacijske naprave, ki se nahajajo zunaj pisarniških prostorov, morajo biti ves čas osebno nadzorovane ali varno shranjene.

(2) Uporabniki prenosnih informacijskih naprav na sredstvih javnega prevoza, v čakalnicah, javnih lokalih in na drugih javnih mestih ne smejo izmenjevati podatkov informacijskega premoženja, ki je uvrščeno v varnostni razred Z1, Z2 ali Z3, ali dostopati do njih, če ne morejo preprečiti prisluhov in vpogledov na zaslon. Na prenosnih informacijskih napravah, ki omogočajo govorno komunikacijo, se ne opravlja zaupnih razgovorov, če se uporabljajo periferne enote z neustrezno zaščiteno ali nezaščiteno brezžično povezavo.

(3) Povezave prek javnih brezžičnih (Wi-Fi) dostopnih točk so omejene na aktivnosti, ki ne vključujejo obravnave podatkov informacijskega premoženja, ki je uvrščeno v varnostni razred Z1, Z2 ali Z3. Za dostop do državnega komunikacijskega omrežja se smejo take povezave uporabljati samo ob upoštevanju določb prejšnjega člena.

(4) Na prenosnih informacijskih napravah, ki imajo vgrajena nezaščitena ali neustrezno zaščitena komunikacijska vrata in hranijo podatke informacijskega premoženja, ki je uvrščeno v varnostni razred Z2 ali Z3, morajo biti ta vrata onemogočena.

IV. PREHODNE IN KONČNE DOLOČBE

1. člen

(roki za izvedbo ukrepov in posredovanje podatkov)

(1) Vlada v šestih mesecih po uveljavitvi te uredbe imenuje odbor iz 3. člena te uredbe.

(2) Upravljavci informacijskih sistemov v dveh letih po uveljavitvi te uredbe zagotovijo nadzorstva iz 38. člena te uredbe.

(3) Organi v enem letu po uveljavitvi te uredbe zagotovijo nadzorstva iz 17. člena te uredbe.

(4) Povezani subjekti v enem letu po uveljavitvi te uredbe zagotovijo nadzorstva iz 17. člena te uredbe.

(5) Organi, ki imajo lastne informacijske sisteme, v enem letu po uveljavitvi te uredbe sprejmejo dokumente iz 13. člena te uredbe.

(6) Predstojniki organov v šestih mesecih po uveljavitvi te uredbe določijo vodje informacijske varnosti in druge odgovorne osebe iz 5. člena te uredbe ter posredujejo imena in kontaktne podatke vodij informacijske varnosti ministrstvu.

(7) Povezani subjekti v šestih mesecih po uveljavitvi te uredbe posredujejo imena in kontaktne podatke koordinatorjev informacijske varnosti ministrstvu.

1. člen

(razveljavitev predpisov)

Z dnem uveljavitve te uredbe prenehajo veljati določbe 68., 70. do 73. in 80. do 91. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07, 31/08, 35/09, 58/10, 101/10 in 81/13).

1. člen

(začetek veljavnosti)

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

Št. xxxxx-x/llll/xx

Ljubljana, xx. meseca 20xx

EVA **2016-3130-0001**

Vlada Republike Slovenije  
 dr. Miroslav Cerar l.r.   
 predsednik

PRILOGA: Razvrstitvena shema s poimenovanjem varnostnih razredov, merila za uvrščanje informacijskega premoženja in sistemov v posamezni varnostni razred ter postopki razvrščanja in označevanja

1. Namen

V tej prilogi je določena in opisana razvrstitvena shema s poimenovanjem varnostnih razredov, opisana so merila za uvrščanje informacijskega premoženja v posamezni varnostni razred ter postopki razvrščanja in označevanja. Varnostni razredi se uporabljajo skupaj z informacijami o ranljivostih in grožnjah pri ocenitvi tveganj za poslovanje organa in za uvedbo ustreznih nadzorstev.

1. Razvrščanje in označevanje informacijskega premoženja in informacijskih sistemov

Vsako informacijsko premoženje in informacijski sistem morata biti razvrščena v varnostni razred. Varnostni razredi se določijo glede na možni učinek, ki bi ga imel na organ dogodek, ki bi ogrozil informacijsko premoženje in informacijske sisteme, ki jih organ potrebuje za uresničevanje svojega poslanstva, varovanje svojega premoženja, izpolnjevanje zakonskih obveznosti, vzdrževanje rednega poslovanja in zaščito posameznikov.

1. Varnostni razredi in varnostni vidiki

Varnostni razredi se nanašajo na vse tri vidike informacijske varnosti: **zaupnost, celovitost in razpoložljivost**.

1. Določanje možnega učinka na organ in posameznike

To navodilo določa tri ravni možnega učinka na organ ali posameznike v primeru ogrožanja ali izgube zaupnosti, celovitosti ali razpoložljivost. Možni učinek je:

**MAJHEN**, če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela omejene negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Omejene** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

* okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij zmanjšana;
* povzročila manjšo škodo premoženju organa (manj kot 100.000 EUR);
* povzročila manjšo finančno izgubo (manj kot 100.000 EUR);
* povzročila manjšo škodo posameznikom (ni potrebna zdravniška oskrba, manj kot dva dni izgube delovnega časa);
* povzročila manjšo škodo ugledu organa (posamične omembe v nekaterih tiskanih, elektronskih in spletnih medijih);

**ZMEREN,** če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela **resne** negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Resne** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

* pomembno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da bi organ sicer lahko izvajal svoje primarne funkcije, vendar bi bila učinkovitost teh funkcij znatno zmanjšana;
* povzročila znatno škodo premoženju organa (od 100.000 EUR do 500.000 EUR);
* povzročila znatno finančno izgubo (od 100.000 EUR do 500.000 EUR);
* povzročila znatno škodo posameznikom, ki pa ne vključuje izgube življenj ali resnih, smrtno nevarnih poškodb (potrebna zdravniška oskrba, do 30 dni izgube delovnega časa);
* povzročila znatno škodo ugledu organa (poročanje v medijih več dni zapored in/ali razprava v DZ);

**VELIK,** če bi izguba zaupnosti, celovitosti ali razpoložljivosti lahko imela **zelo resne ali katastrofalne** negativne posledice za poslovanje organa, premoženje organa ali posameznike. **Zelo resne ali katastrofalne** negativne posledice pomenijo, da bi izguba zaupnosti, celovitosti in razpoložljivosti lahko:

* močno okrnila zmožnost opravljanja poslanstva v takem obsegu in trajanju, da organ ne bi mogel izvajati ene ali več svojih primarnih funkcij;
* povzročila veliko škodo premoženju organa (nad 500.000 EUR);
* povzročila veliko finančno izgubo (nad 500.000 EUR);
* povzročila zelo resno ali katastrofalno škodo posameznikom, ki vključuje izgubo življenj ali resne, smrtno nevarne poškodbe (množične poškodbe in smrtne žrtve);
* povzročila veliko škodo ugledu organa (večtedensko poročanje v medijih in/ali razprava o ukrepih v DZ).

1. Varnostno razvrščanje informacijskega premoženja

Varnostni razred posameznega informacijskega premoženja je lahko povezan tako z uporabniškimi kot sistemskimi informacijami in se lahko nanaša na informacije v elektronski ali neelektronski obliki. Določitev ustreznega varnostnega razreda posameznega informacijskega premoženja zahteva določitev možnega učinka (na podlagi treh varnostnih vidikov), ki je povezan s tem informacijskim premoženjem.

Posplošeni zapis, s katerim izrazimo varnostni razred (VR) informacijskega premoženja (IP), je:

VRIP = {(zaupnost, *učinekIP*), (celovitost, *učinekIP*), (razpoložljivost, *učinekIP*)}

kjer so vrednosti za možni učinek lahko: MAJHEN, ZMEREN, VELIK ali SNU[[1]](#footnote-1) (se ne uporablja).

1. Varnostno razvrščanje informacijskih sistemov

Za določitev varnostnega razreda informacijskega sistema je treba analizirati in upoštevati vse varnostne razrede informacijskih premoženj, ki se nahajajo v informacijskem sistemu. Vrednosti možnega učinka, dodeljene informacijskemu sistemu na podlagi vseh treh varnostnih vidikov (zaupnost, celovitost, razpoložljivost), morajo biti najvišje vrednosti varnostnih razredov, ki so bili določeni za vsako posamezno informacijsko premoženje, ki se nahaja v tem informacijskem sistemu.

Posplošeni zapis, s katerim izrazimo varnostni razred (VR) informacijskega sistema (IS), je:

VRIS = {(zaupnost, *učinekmax(IPi)*), (celovitost, *učinekmax(IPi)*), (razpoložljivost, *učinekmax(IPi)*)}

kjer so vrednosti za možni učinek lahko: MAJHEN, ZMEREN ali VELIK.

Pri določanju varnostnih razredov informacijskih sistemov vrednosti SNU ni mogoče dodeliti nobenemu varnostnemu vidiku, saj mora obstajati najmanj MAJHEN možni učinek ob izgubi zaupnosti, celovitosti in razpoložljivosti informacijskega sistema zaradi temeljne zahteve po varovanju sistemskih procesnih funkcij in ključnih informacij za delovanje informacijskega sistema.

1. Označevanje varnostnih razredov

Na podlagi določitve varnostnega razreda označimo posamezno informacijsko premoženje oziroma informacijski sistem, kot sledi:

| Varnostni razred | Oznaka (kratka oznaka) | Varnostne zahteve |
| --- | --- | --- |
| ZAUPNOST | | |
| (zaupnost, MAJHEN) | Z: NOTRANJE (Z1) | Dostop omejen na uslužbence organa |
| (zaupnost, ZMEREN) | Z: OMEJENO (Z2) | Dostop omejen na tiste uslužbence organa, ki jih to zadeva |
| (zaupnost, VELIK) | Z: STROGO OMEJENO (Z3) | Dostop omejen na tiste prepoznane uslužbence organa, ki to morajo vedeti |
| CELOVITOST | | |
| (celovitost, MAJHEN) | C: UGOTOVLJIVA (C1) | Celovitost je lahko okrnjena, vendar je okrnjenost mogoče prepoznati |
| (celovitost, ZMEREN) | C: NADZOROVANA (C2) | Celovitost je lahko okrnjena, če je okrnjenost mogoče prepoznati in celovitost obnoviti |
| (celovitost, VELIK) | C: POPOLNA (C3) | Zahteva se popolna neokrnjenost |
| RAZPOLOŽLJIVOST | | |
| (razpoložljivost, MAJHEN) | R: OBČASNA (R1) | Nerazpoložljivost več kot 24 ur |
| (razpoložljivost, ZMEREN) | R: PRETEŽNA (R2) | Nerazpoložljivost največ 24 ur |
| (razpoložljivost, VELIK) | R: STALNA (R3) | Razpoložljivost brez prekinitev |

Oznaka odraža tudi varnostne zahteve za posamezni varnostni razred glede na posamezne vidike informacijske varnosti.

1. Pregled opredelitev možnih učinkov

V spodnji tabeli so povzete opredelitve možnih učinkov za vsak varnostni vidik: zaupnost, celovitost in razpoložljivost.

|  |  |  |  |
| --- | --- | --- | --- |
| MOŽNI UČINEK | | | |
| **Varnostni vidik** | **MAJHEN** | **ZMEREN** | **VELIK** |
| ***Zaupnost –***  lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim posameznikom, entitetam ali procesom. | Nepooblaščeno razkritje informacij ima lahko **omejene**  negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **Z: NOTRANJE (Z1)** | Nepooblaščeno razkritje informacij ima lahko **resne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **Z: OMEJENO (Z2)** | Nepooblaščeno razkritje informacij ima lahko **zelo resne ali katastrofalne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **Z: STROGO OMEJENO (Z3)** |
| ***Celovitost –***  lastnost informacij in informacijskih sistemov, da so točni in popolni. | Nepooblaščena sprememba ali uničenje informacij in informacijskih sistemov ima lahko **omejene** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **C: UGOTOVLJIVA (C1)** | Nepooblaščena sprememba ali uničenje informacij in informacijskih sistemov ima lahko **resne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **C: NADZOROVANA (C2)** | Nepooblaščena sprememba ali uničenje informacij in informacijskih sistemov ima lahko **zelo resne ali katastrofalne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **C: POPOLNA (C3)** |
| ***Razpoložljivost –***  lastnost informacij in informacijskih sistemov, da so dostopni in uporabni na zahtevo pooblaščene entitete. | Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko **omejene** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **R: OBČASNA (R1)** | Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko **resne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **R: PRETEŽNA (R2)** | Motnje ali prekinitve dostopa do informacij ali uporabe informacijskega sistema ima lahko **zelo resne ali katastrofalne** negativne učinke na poslovanje organa, premoženje organa ali posameznike.  **R: STALNA (R3)** |

1. Za informacijsko premoženje, ki obsega javne informacije, se npr. možni učinek z vidika zaupnosti ne uporablja (SNU) [↑](#footnote-ref-1)