Pronid
Informacijska Tehnologija

INFORMACIJSKA VARNOSTNA POLITIKA (IVP) – DD Drava

Pripravil:

Marjan Gomolj

Maribor, 31. 3. 2016

INFORMACIJSKA VARNOSTNA POLITIKA (IVP) – DD Drava

1. Namen in cilji

1. člen

Informacijska varnostna politika (IVP) izraža politiko, s katero želi DD Drava Maribor zaščititi informacijsko premoženje, ki ga upravlja.

IVP dokument, ki ga morajo upoštevati vodstvo, zaposleni, osebe pogodbenega izvajalca (upravitelja) in vsi, ki imajo dostop do tega informacijskega premoženja.

2. člen

Namen IVP je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi nevarnostmi. Izvajanje te politike je pomembno za zagotavljanje informacijske varnosti.

Informacijsko varnost označujemo kot varovanje:

- zaupnosti: varovanje podatkov in informacij pred razkritjem nepooblaščenim ter zagotavljanje odgovornosti za njihova dejanja;
- celovitosti: varovanje podatkov in informacij pred neavtoriziranimi spremembami, zagotavljanje verodostojnosti – točnosti, popolnosti in nespremenljivosti informacij ter postopkov procesiranja;
- razpoložljivosti: varovanje podatkov, informacij in servisov pred prekinitvami v delovanju ter zagotavljanje informacij pooblaščenim uporabnikom v času, ko jih potrebujejo, in na zahtevani način.

V IVP uporabljeni izrazi ravnatelj, zaposleni in drugi izrazi, zapisani v moški slovnični obliki, so zapisani kot nevtralni izrazi za moške in ženske.

3. člen

Z IVP se zagotavlja doseganje naslednjih temeljnih ciljev:

- zavarovanje podatkov/informacij pred nepooblaščenim dostopom, obdelavo in razkritjem,
- ohranitev celovitosti informacij in preprečevanje nepooblaščenih sprememb,
- razpoložljivost informacij in virov, ko jih pooblaščeni potrebujejo,
- priprava, vzdrževanje in preverjanje načrtov neprekinjenega poslovanja v obsegu, ki je praktično izvedljiv,
- izobraževanje o informacijski varnosti,
- beleženje in raziskovanje kršitev IVP in sum teh kršitev,
- preverjanje skladnosti z zakonodajo,
- upoštevanje priporočil glede standardov informacijske varnosti.

4. člen

Vsakdo mora upoštevati IVP v okviru njegovih delovnih naloge ali pogodbene obveznosti.

Zaposleni se seznanijo z IVP preko objave na spletni strani DD Drava. Pogodbeni izvajalci se pred opravljanjem nalog seznanijo z IVP in podpišejo izjavo o seznanitvi z IVP.

2. Politika fizičnega varovanja

Fizični dostop

5. člen

DD Drava Maribor mora poskrbeti za ustrezno varovanje svojih prostorov.

6. člen

V upravne prostore je obiskovalcu dovoljen vstop v delovnem času samo v spremstvu.

7. člen

Prostori, v katerih se obravnavajo podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do informacijske in komunikacijske tehnologije za podatkovno obdelavo.

8. člen

Dostop zaposlenim na varovano območje je mogoč le v rednem delovnem času, zunaj tega časa pa samo na podlagi dovoljenja nadrejenega.

3. Varovanje sredstev za dostop

9. člen

Vsak zaposleni mora fizična sredstva (ključe, itd.) in elektronska sredstva (uporabniška imena, gesla, itd.) za dostop do območij in opreme varno in skrbno hraniti, jih imeti vedno pod nadzorom in jih ne sme posojati. Podatki za dostop se štejejo za občutljive podatke.

10. člen

Morebitno krajo, izgubo ali založitev sredstva za dostop mora vsak takoj prijaviti izdajatelju tega sredstva.

Varovanje in namestitev opreme

11. člen

Vsa oprema mora biti nameščena in zaščitena tako, da so nevarnosti iz okolja in priložnosti za nepooblaščeni dostop kar najbolj odpravljene.

12. člen

Raven varovanja in zaščite je določena glede na občutljivost podatkov in ocenjeno tveganje izgube ali poškodovanja podatkov.

Protipožarno varovanje

13. člen

Protipožarno varovanje na varovanih območjih, na katerih je nameščena ključna in pomožna oprema, mora biti izvedeno skladno s predpisi, ki urejajo to področje, in navodili ustreznih pooblaščenih služb.

Zaščita ožičenja

14. člen

Ožičenje morajo vedno načrtovati in nameščati ustrezno usposobljeni izvajalci ter mora biti izvedeno skladno z veljavnimi standardi in predpisi ter priporočili naročnika.

Varnost ožičenja je treba načrtovati že pri vzpostavljanju računalniških prostorov in tako pri namestitvi opreme.

15. člen

Električni in telekomunikacijski kabli (ožičenje), po katerih se prenašajo podatki oziroma, ki podpirajo informacijske storitve, morajo biti zaščiteni pred prestrezanjem ali poškodbami.

16. člen

Vsi priključki morajo biti dokumentirani. Posebej morajo biti dokumentirani porabljeni oziroma aktivni priključki, bodisi na aktivni opremi bodisi na priključnih panojih. Prosti priključki v sobah in hodnikih ne smejo omogočati nepooblaščenega dostopa, zato morajo biti »neaktivni« ali blokirani.

17. člen

Popravila na ožičenju lahko izvajajo samo skrbniki omrežja ali pod njihovim nadzorom strokovno usposobljeni izvajalci.

4. Politika primerne rabe informacijskih sistemov in zaščite občutljivih podatkov

Uporaba opreme informacijske tehnologije

18. člen

Informacijska oprema je namenjena opravljanju oziroma potrebam dela v DD Drava Maribor. Uporaba v zasebne namene ni dovoljena.

19. člen

Zaposleni morajo z informacijsko opremo ravnati skrbno, po priporočilih proizvajalca in skrbnika sistema. Posege vanjo lahko opravljajo samo za to pooblaščene osebe.

20. člen

Za odtujitev in poškodbe opreme je odgovoren zaposleni. Posebno skrbno mora ravnati s prenosno opremo.

21. člen

Zaposleni ne smejo sami nameščati programske opreme razen z dovoljenjem odgovorne osebe. Nameščanje in vzdrževanje te opreme je v domeni skrbnikov informacijskih sistemov. Upravljavci informacijskih sistemov morajo poskrbeti, da so informacijski sistemi ustrezno zaščiteni pred neavtorizirano ali zlonamerno programsko opremo. Nameščeni morajo biti vsaj protivirusni programi in požarni zid. Zagotovljeno mora biti redno posodabljanje teh programov.

Zlonamerna programska oprema

22. člen

Nameščanje ali uporaba zlonamerne programske opreme ali njeno širjenje je kršitev varnostne politike. Namerno nameščanje, uporaba in širjenje take opreme se preganja v skladu z relevantno zakonodajo in internimi akti.

Uporabniki računalniške opreme:

- morajo, če sumijo, da na informacijskem sistemu deluje zlonamerna programska oprema, takoj nehati delati z njim, obvestiti pristojno osebo in upoštevati njegova navodila;
- morajo, če sumijo, da je na informacijskem sistemu zlonamerna programska oprema, takoj obvestiti pristojno osebo in upoštevati njegova navodila;
- ne smejo zaganjati izvršljive programske opreme, ki ni del njihovega informacijskega sistema (izvira npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev);
- ne smejo zaganjati dokumentov (npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev), če so sumljivi, če ne vedo, čemu so takšni dokumenti ali programi namenjeni, ali če ne poznajo njihovega izvora;

- morajo, če sumijo ali ugotovijo, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, takoj nehati uporabljati informacijski sistem, obvestiti nadrejenega in upoštevati njegova navodila;

Informacijski sistemi

23. člen

Informacijski sistemi, ki obravnavajo občutljive podatke, morajo biti nadzorovani. Nadzirajo se lahko tudi sistemi, ki obravnavajo druge podatke. V nadzorovanih sistemih morajo biti vključeni ustrezni dnevniki, ki zagotavljajo spremljanje dogodkov.
Dnevniki morajo omogočiti identifikacijo uporabnika, ki je bodisi vpogledoval v podatke ali jih spreminjal. Tudi izpis ali izvoz podatkov iz dnevnikov mora ostati pod nadzorom in nespremenjen.

Podatke iz dnevnika je mogoče pridobiti le na pisno zahtevo predstojnika organa ali zahtevo pristojnega preiskovalnega organa v zvezi s sumom storitve kaznivega dejanja.

Podatki iz dnevnika se uporabljajo tudi za odkrivanje napak v informacijskem sistemu ali za izboljšanje njegovega delovanja. V tem primeru soglasje ni potrebno.
V primeru, da dnevniki vsebujejo občutljive podatke morajo biti zabeleženi vpogledi in ostali posegi na sistemu.

24. člen

Uporaba zasebne opreme v informacijskem sistemu DD Drava Maribor ni dovoljena.

Upravljanje izmenljivih nosilcev podatkov

25. člen

Zaposleni mora varovati in zaščititi izmenljive nosilce podatkov.

26. člen

Izgubo ali krajo izmenljivih nosilcev podatkov je treba prijaviti odgovorni osebi.

27. člen

Nosilci podatkov neznanega ali sumljivega izvora se ne smejo uporabljati. Preden se uporabi vsebina izmenljivega nosilca podatkov, se mora vselej preveriti njegova morebitna okuženost z zlonamerno programsko opremo.

28. člen

Uporabnik mora vse nosilce podatkov, ki jih ne potrebuje več oziroma so neuporabni, izročiti odgovorni osebi.

Dostop do informacijskih sistemov

29. člen

Za vsak informacijski sistem mora biti vzpostavljen postopek dodelitve, sprememb in prenehanja dostopnih pravic. Dostop do podatkov v računalniškem sistemu se varuje z gesli.

30. člen

Dostop do posameznih informacijskih sistemov in njegovih delov smejo imeti samo osebe, ki so do tega upravičene, za to pooblaščene in ustrezno usposobljene.

31. člen

Na podlagi potreb poslovnega procesa se odobri dostop do informacijskega sistema v obsegu, ki je potreben za opravljanje delovnih nalog.

34. člen

Dostop do informacijskih sistemov mora biti mogoč le na podlagi ustrezne avtentikacije, minimalno z uporabo uporabniškega imena in gesla. Za prijavo v sistem se lahko poseže še po drugih odobrenih avtentikacijskih metodah.

32. člen

Sredstva za dostop do informacijskega sistema so neprenosljiva. Posojanje ni dovoljeno.

33. člen

Uporabnik mora skrbno varovati sredstva za dostop do informacijskih sistemov, da se ne odtujijo ali zlorabijo. Vsak sum zlorabe ali odtujitve je treba takoj prijaviti skrbniku sistema.

34. člen

Dostop do storitev in upravljanja informacijskih sistemov ter omrežja je mogoč po sistemu pravic. Te dodeljuje upravljavec informacijskega sistema ali omrežja ali pa v njegovem imenu izvajalec.

35. člen

Pravico dostopa do informacijskega sistema ali omrežja lahko pridobijo zaposleni ali administratorji na podlagi potrebe in odobritve lastnika aplikacije ali storitve. Če potreba po dostopu preneha, je treba to pravico odvzeti. Spremembe dostopnih pravic se morajo voditi v personalni mapi v organizacijski enoti, pristojni za upravljanje človeških virov.

Postopek upravljanja pravic dostopa do informacijskega sistema mora biti dokumentiran, dodeljene pravice pa redno pregledovane.

39. člen

Uporabniške in administratorske pravice dostopa do informacijskih sistemov so ločene.

36. člen

Preverjanje informacijske varnosti v informacijskih sistemih s pomočjo penetracijskih testov, ki se izvajajo iz prostranega omrežja, se lahko izvaja izključno s pisnim soglasjem upravljavca prostranega omrežja. Naročnik testa je z rezultati dolžan seznaniti tudi upravljavca omrežja.

Načelo čiste mize

37. člen

Zaposleni ne smejo puščati nosilcev podatkov (npr. v papirni obliki, elektronskih medijev) z občutljivimi podatki na odprtih površinah pisarniške opreme ali drugih mestih, kjer bi lahko bili dostopni nepooblaščenim osebam. Ko zaposlenega ni v prostoru, morajo biti nosilci podatkov varno shranjeni.

38. člen

Zunaj delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov, ki niso javni, zaklenjena ali drugače varovana, komunikacijsko-informacijska oprema pa fizično ali programsko varovana.

Načelo praznega zaslona

39. člen

Ob uporabnikovi prisotnosti ali odsotnosti na delovnem mestu mora biti onemogočen vpogled na zaslon oziroma onemogočena uporaba informacijsko-komunikacijske opreme nepooblaščenim osebam:

- delovna mesta morajo biti organizirana tako, da se prepreči priložnostno "gledanje čez rame";
- uporabljati se mora oprema, ki po določenem času uporabnikove neaktivnosti na delovni postaji izključi zaslon ali ga preklopi na ohranjevalnik zaslona, zavarovan z geslom;
- ob koncu delovnega procesa se je treba odjaviti iz sistema in izklopiti delovno postajo, razen če ni z drugim navodilom določeno drugače.

Oddaljeni dostop

40. člen

Oddaljeni dostop do informacijskega sistema je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer za tiste zaposlene, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar le v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da občutljivi podatki in sledi ne ostanejo na delovni postaji.

41. člen

Za uveljavitev oddaljenega varnega dostopa je na strojni opremi zagotovljena prepoznava ustrezne programske opreme, ki omogoča zaščito končne točke pred internetnimi grožnjami.

Za zagotavljanje zaupnosti se ves promet iz končne točke oddaljenega omrežja do omrežja DD Drava Maribor uprave šifrira.

42. člen

Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

43. člen

Zaposleni morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki njenih informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom organa DD Drava Maribor.

44. člen

Na podlagi ocene tveganja je mogoče omejevati dostop do vsebin zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev etičnih in moralnih norm.

45. člen

Pošiljanje službenih elektronskih naslovov na zunanje spletne strežnike ni dovoljeno, razen če je povezano s poslovnim procesom organa DD Drava Maribor.

46. člen

V omrežju DD Drava Maribor se lahko za namen preiskave suma nezakonitih dejanj beležijo dostopi uporabnikov do spletnih strani in s tem povezani podatki o dodeljenih internih IP številkah, času dodelitve interne IP številke ter podatki o povezavi med interno in javno IP

številko. Te podatke lahko zaposleni posredujejo le na obrazloženo zahtevo organa, ki na podlagi zakonskih pooblastil obravnava domnevno nezakonita dejanja.
Drugačna obdelava podatkov iz prvega stavka ni dovoljena.

47. člen

Zaposleni v DD Drava Maribor kot orodje za komunikacijo s strankami, zaposlenimi in zunanjimi izvajalci uporabljajo tudi elektronsko pošto. Pri tem se morajo držati ne le etičnih in moralnih norm, temveč tudi bontona. Vsi uporabniki morajo imeti dostop do elektronske pošte, varovan z geslom.

Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje organa, v katerem je pošiljatelj zaposlen.

48. člen

Sistem elektronske pošte se uporablja samo v službene namene.

49. člen

Uporabniki po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, prezentacije, zagonske datoteke in skripte…), razen če so namenjene delu. Pošiljanje obvestil o morebitnih novih virusih ni dovoljeno niti takrat, ko so prepričani, da ne gre za lažna obvestila. Sumljivo pošto naj pošljejo izključno pooblaščenim osebam.

50. člen

Zaposleni svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove. Če imajo potrebo po pošiljanju elektronske pošte večjemu številu naslovnikov, se morajo pred pošiljanjem posvetovati s skrbnikom poštnega sistema. Vsa elektronska sporočila, ki so bila poslana velikemu številu naslovnikov iz imenika in s pošiljanjem katerih upravitelj imenika ni bil predhodno seznanjen, se štejejo za neželeno pošto, in bodo zavrnjena.

Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi, razen če to ni povezano s potrebami delovnega mesta.

51. člen

Uporabniki morajo biti previdni pri odpiranju pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi bila lahko škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo skrbnika poštnega sistema.

52. člen

Uporabniki nikakor ne smejo pošiljati občutljivih podatkov ali gesel po elektronski pošti razen v ustrezno akreditiranih sistemih.

53. člen

S službenimi elektronskimi sporočili je treba ravnati v skladu z veljavnimi pravili poslovanja z dokumentarnim gradivom.

Za prijavo na dogodke in za sporočila, povezana z opravljanjem delovnih nalog, ni dovoljeno uporabljati zasebnih elektronskih naslovov. Službene elektronske pošte tudi ni dovoljeno preusmerjati na druge zasebne naslove.

Pravice nad podatki elektronske pošte

54. člen

Vse pravice na sistemu elektronske pošte in vseh elektronskih sporočilih pripadajo organu DD Drava Maribor.

55. člen

Uporabnik ne sme uporabljati elektronskega poštnega naslova, ki je bil dodeljen drugemu uporabniku.

56. člen

V primeru ukinitve elektronskega poštnega naslova se pošiljateljem elektronskih sporočil na ukinjeni elektronski poštni naslov, pošlje sporočilo o nedostopnosti elektronskega poštnega naslova in po možnosti obvestilo o nadomestnem naslovu. Sprejemanje elektronskih sporočil na ukinjeni elektronski poštni naslov se onemogoči. Vsebina poštnega predala do ukinitve elektronskega poštnega naslova se arhivira skladno z relevantno zakonodajo. Preusmeritev elektronske pošte v drug predal uporabnika ni dovoljena.

57. člen

Elektronska sporočila, ki jih sprejme uporabnik na svoj elektronski poštni naslov, sme odpirati samo ta uporabnik, ali s strani uporabnika pooblaščena oseba, drug uporabnik pa samo na podlagi odredbe nadrejenega. Pri tem se morajo upoštevati določila relevantne zakonodaje in vsa pravila, ki v takšnih primerih veljajo za ravnanje z gesli.

Privzete nastavitve predala

58. člen

Zaposleni ne sme spreminjati nastavitev svojega elektronskega poštnega predala. Za uporabo dodatnih pripomočkov mora pridobiti posebno dovoljenje oziroma odobritev upravitelja.

Velikost elektronskih sporočil

59. člen

Največja velikost sporočil pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena. Omejitev določa upravljavec elektronske pošte. Če je omejitev presežena, se sporočilo samodejno zavrne, pošiljatelj pa dobi obvestilo o zavrnitvi.

60. člen

Če zaposleni prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega sporočila ne sme shraniti ali kakor koli uporabiti. O tej pomoti mora obvestiti pošiljatelja, sporočilo pa mora nemudoma izbrisati ali kako drugače uničiti. Pred uničenjem ga lahko pošlje pravemu naslovniku, če je iz sporočila nedvoumno razvidna njegova identiteta.

61. člen

Čeprav upravitelj zagotavlja zaupnost, se mora vsak zaposleni zavedati, da elektronsko pošto lahko, odvisno od tehnologije, prestrežejo in obdelujejo nepooblaščene osebe.

62. člen

Zaposleni mora spoštovati avtorske pravice in pravila intelektualne lastnine, še zlasti tako, da ne uporablja sistema elektronske pošte za pošiljanje avtorsko zaščitenih informacij ali računalniških programov.

63. člen

Pri ravnanju z občutljivimi podatki je treba dosledno upoštevati veljavno zakonodajo.

Šifriranje in podpisovanje elektronskih sporočil

64. člen

Šifriranje in podpisovanje elektronskih sporočil se lahko izvaja samo z uporabo odobrenih metod v organu DD Drava Maribor.

Brisanje elektronskih sporočil

65. člen

Vsak zaposleni mora vsa elektronska sporočila, ki jih ne potrebuje več, občasno brisati iz svojega predala oziroma mora to storiti na zahtevo upravitelja. Pri shranjevanju elektronskih sporočil morajo zaposleni upoštevati načelo racionalnosti in se izogibati hranjenju dokumentov v multimedijskih podatkovnih formatih, ki zavzamejo veliko prostora (filmi, slike visoke resolucije, zvočni zapisi).

66. člen

Nezaželeno pošto ima upravitelj pravico brisati.

Posebna pooblastila

67. člen

Za varno in nemoteno delovanje sistema elektronske pošte skrbijo upravitelji lokalnega sistema in upravitelji elektronskih poštnih strežnikov.

68. člen

Ob sumu storitve kaznivega dejanja z uporabo elektronskih sporočil, se opravijo postopki skladno z relevantno zakonodajo po odredbi pristojnega organa.
Pregledovanje elektronskih sporočil upravljavcev elektronske pošte iz radovednosti ali po nalogu nepooblaščenih posameznikov ni dovoljeno.

Dostop do podatkov

69. člen

Vzpostavljeni morajo biti mehanizmi, ki preprečujejo nepooblaščeni dostop do podatkov, ter organizacijski in tehnični postopki, ki preprečujejo nepooblaščeno obdelavo podatkov, vključno s spreminjanjem oziroma uničenjem.

70. člen

Upravljavci informacijskih sistemov ne smejo imeti vpogleda v občutljive podatke, razen če imajo za to ustrezna pooblastila.

71. člen

Dostop do zbirk občutljivih podatkov v elektronski obliki mora biti zaščiten z ustreznimi dostopnimi pravicami (npr. prijavno ime in geslo, certifikat in geslo, enkratno geslo, biometrija).

72. člen

Dostopne pravice morajo biti urejene tako, da omogočajo posamezniku dostop do najmanjšega možnega nabora podatkov, ki so potrebni za opravljanje nalog.

73. člen

Uporabniška imena, gesla, kartice za preverjanje dostopa, certifikati in drugi odobreni dostopni mehanizmi ter s tem pridobljene pravice dostopa do informacijskih sistemov in zbirk občutljivih podatkov so vedno izdani na eno osebo in so neprenosljivi.

Posojanje uporabniških imen, gesel, kartic za preverjanje dostopa, certifikatov in drugih odobrenih dostopnih mehanizmov ni dovoljeno.

74. člen

Prostori, v katerih se obravnavajo podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov in sredstev informacijske tehnologije, s katero se slednji obdelujejo.

75. člen

Pri elektronskih zbirkah občutljivih podatkov morajo biti izpolnjeni organizacijsko- tehnični pogoji za vzdrževanje teh zbirk ter zagotovljeni postopki za varnostno shranjevanje in arhiviranje teh podatkov skladno z relevantno zakonodajo.

76. člen

Zaposleni morajo varovati občutljive podatke, s katerimi so se seznanili med trajanjem delovnega razmerja. Varovati jih morajo tudi po prenehanju delovnega razmerja.

5. Politika razvoja in vzdrževanja informacijskih sistemov in obvladovanja sprememb

Načrtovanje

77. člen

Med načrtovanjem in vzpostavitvijo informacijskih sistemov ter njihovih posameznih delov je treba vgraditi ustrezne mehanizme za avtentikacijo in avtorizacijo uporabnikov, ustrezno sledljivost in druge elemente za zaščito podatkov.

78. člen

Uporabljati je treba preverjene tehnologije, ki omogočajo vzpostavitev varnega in stabilnega informacijskega okolja.

79. člen

Novi informacijski sistemi morajo biti skladni z varnostno shemo v omrežju DD Drava Maribor.

80. člen

Kakršne koli spremembe v informacijskem sistemu smejo biti izvedene le na podlagi naročila lastnika sistema. Postopek upravljanja sprememb in same spremembe morajo biti dokumentirane.

6. Politika upravljanja informacijskega sistema

81. člen

Naloga upravljavca informacijskega sistema je, da poskrbi za njegovo delovanje z zagotavljanjem varnosti (zanesljivost, celovitost in razpoložljivost).

82. člen

Za omrežje in njegovo varnost je zadolžen skrbnik omrežja. Ta stalno preverja nespremenljivost omrežja in njegovo skladnost z dokumentacijo.

Skrbnik omrežja preverja fizične in logične nastavitve njegovih gradnikov in omrežja samega ob spremembah ali najmanj enkrat na leto.

Nadzor dostopa do omrežja

83. člen

Sistem za diagnostiko omrežnih naprav in postopki njihove konfiguracije morajo biti ustrezno nadzorovani.

Upravljanje omrežnega usmerjanja

84. člen

Vzpostavljen mora biti sistem nadzora nad delovanjem informacijskih sistemov. Vsak od njih mora vključevati postopek obveščanja zaradi morebitnih izpadov in težav v delovanju, pa tudi postopek obveščanja po odpravi težav.

Oskrba z električno energijo

85. člen

Ključna oprema in pomožne informacijske naprave morajo biti priključene na sisteme prekinjenega napajanja (UPS).

Klimatski pogoji

86. člen

Ključna informacijsko-komunikacijska oprema mora biti nameščena v prostorih z ustreznimi klimatskimi razmerami, ki jih zahtevajo standardi za opremo.

Varnostne kopije

87. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema se dnevno zagotavlja redna izdelava kopij vsebine osebnih podatkov iz strežnika, preko mrežne povezave na enoto za shranjevanje podatkov.

88. člen

Kopije vsebin osebnih podatkov na strežniku se hranijo na enoti za shranjevanje podatkov.

89. člen

Varnostne kopije podatkov v informacijskem sistemu morajo biti izdelane, hranjene in preverjane skladno z zahtevami upravljavca informacijskega sistema.
Zahteve vsebujejo informacijo o podatkih, ki naj jih vsebuje varnostna kopija, in o pogostnosti izdelave teh kopij. Postopek izdelave varnostnih kopij in njihove ponovne uporabe mora biti dokumentiran.

Samodejni postopki izdelave varnostnih kopij morajo biti ustrezno preverjeni pred uporabo in v rednih obdobjih.

90. člen

Varnostne kopije zahtevajo enake varnostne pogoje kakor delujoča zbirka podatkov. Po potrebi morajo biti podatki šifrirani.

Upravljanje neprekinjenega poslovanja

91. člen

Poslovni procesi v DD Drava Maribor, ki so podprti z informacijskimi sistemi, lahko imajo dokumentiran postopek – načrt neprekinjenega poslovanja, ki opredeljuje:

- oceno škodljivih posledic ob morebitnem izpadu informacijskega sistema, omrežja ali infrastrukture,
- odzivni čas ob izpadu in čas odprave napake,
- načrt za vzpostavitev informacijskega sistema po izpadu,
- zahtevo po izdelovanju varnostnih kopij podatkov in programske opreme informacijskega sistema,
- kontaktne podatke in odgovornost oseb za obveščanje in ukrepanje ter
- druge potrebne sestavine za vzpostavitev podpore poslovnim procesom.

92. člen

Skrbniki načrtov neprekinjenega poslovanja so lastniki procesov. Vsaka pogodbena stranka, ki ima sklenjeno pogodbo z DD Drava mora skrbeti za ažurnost podatkov v prejšnjem členu in slediti smernicam neprekinjenega poslovanja v primeru katastrofalnega dogodka.

93. člen

Vodstvo s skrbniki določi prednostne naloge pri reševanju informacijskih sistemov ob morebitni večji katastrofi.

94. člen

Skrbniki informacijskih sistemov morajo redno vzdrževati produkcijsko okolje in omogočati njegovo neprekinjeno delovanje.

Vodstvo in skrbniki skupaj načrtujejo razvoj infrastrukture in zagotavljajo vire za njeno nemoteno delovanje.

Vzdrževanje opreme

95. člen

Za vso opremo mora biti zagotovljeno vzdrževanje, ki ga lahko opravljajo pooblaščeni izvajalci.

Vzdrževalna dela

96. člen

Pri načrtovanih vzdrževalnih delih na programski ali komunikacijski opremi morajo upravitelji predhodno obvestiti uporabnike o morebitnih motnjah, niso pa odgovorni za motnje, ki nastanejo zunaj njihove pristojnosti.

7. Kršitev politike

97. člen

V informacijskem sistemu mora biti zagotovljeno zaznavanje kršitev IVP (nepooblaščen dostop, posredovanje podatkov nepooblaščenim osebam,…) in njihovo sankcioniranje v skladu z IVP in internimi akti.

98. člen

Pogodbeni izvajalec ima pravico do takojšnje blokade in morebitne naknadne ukinitve storitve (dostop do el. pošte, interneta, podatkov na strežniku), če se ugotovi kršitev določil IVP.

99. člen

V primeru kršitev IVP se zoper kršitelja uvedejo postopki skladno z določili Zakona o delovnih razmerjih in kolektivnih pogodb ter internih aktov.

8. Končna določba

100.člen

IVP velja od objave dne ….. Šteje se, da so z dnem objave seznanjeni vsi zaposleni v DD Drava Maribor.

Ravnatelj
Ivan Sagadin