Na podlagi 80. 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) ter Priporočil informacijske varnostne politike javne uprave (št. 386-2/2008/23 z dne 28.10. 2010) izdajam

INFORMACIJSKO VARNOSTNO POLITIKO V ZGODOVINSKEM ARHIVU NA PTUJU

Namen in cilji

1. člen

Informacijska varnostna politika javnega zavoda Zgodovinskega arhiva na Ptuju (IVPZAP) izraža politiko, s katero želi zaščititi informacijsko premoženje, ki ga upravlja ali uporablja. Je dokument, ki ga morajo upoštevati vodstvo, zaposleni, osebe pogodbenih izvajalcev in vsi, ki imajo dostop do tega premoženja.

2. člen

Namen IVPZAP je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. 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.

3. člen

Z IVPZAP 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 IVPZAP in sum teh kršitev,
- preverjanje skladnosti z zakonodajo,
- upoštevanje priporočil glede standardov informacijske varnosti.

Uporabljeni izrazi

4. člen

digitalno potrdilo – potrdilo, ki vsebuje podatke o identiteti imetnika, izdajatelja in imetnikov javni ključ, s katerim se overi elektronski podpis;
dogodek – stanje ali sprememba, ki lahko vpliva na informacijsko varnost;
dokumentacija – vsi pisni ali elektronski podatki o opremi ali postopkih;
elektronska pošta – storitev za izmenjavo elektronskih sporočil;
elektronski poštni predal – zbirka podatkov, v kateri se shranjujejo elektronska sporočila uporabnika ali namenske skupine uporabnikov, prejeta ali poslana po sistemu elektronske pošte;
elektronsko sporočilo – niz podatkov, ki so poslani ali prejeti po elektronski poti;
incident – dogodek, katerega posledica je razkritje, uničenje, nerazpoložljivost podatkov ali informacijskega sistema in kršitev varnostne politike
informacijski sistem (IS) – celoten skupek opreme (komunikacijske in informacijske) in postopkov za obravnavanje podatkov organa javnega zavoda;
informacijski varnostni dogodek – vsak dogodek, ki lahko vpliva na varnost podatkov v informacijskem sistemu ali na delovanje informacijskega sistema;
infrastruktura – energetski in komunikacijski vodi, generatorji, klimatske naprave, sistemi neprekinjenega napajanja (sistemi UPS), sistemi za gašenje, prostori …;
izmenljivi nosilci podatkov – nosilci podatkov, ki jih je mogoče z enostavnim posegom odstraniti in ločiti od IS. Sem sodijo diskete, trakovi, CD- in DVD-mediji, USB-pomnilniki in diski;
kriptografija – proučevanje in uporaba šifriranja in dešifriranja podatkov, sporočil;
kriptografske kontrole – preverjanje, določanje in upravljanje kriptografskih ključev;
kriptografski ključi – niz znakov, ki so vhodni podatek za izvedbo šifrirnega algoritma;
kritična infrastruktura – oprema, ki je nujno potrebna za delovanje minimalnih funkcij javnega zavoda;
lokalno omrežje (LAN) – računalniško omrežje z aktivnimi in pasivnimi elementi, ki omogoča povezljivost ter pretok podatkov med terminalsko opremo in viri v organizaciji ali organizacijski enoti;
nepooblaščeni dostop – nedovoljen dostop do prostorov, podatkov in informacij, dostop brez ustreznega pooblastila;
nezavarovano območje – bakreni ali optični vodi, ki potekajo prek javnih prostorov med stavbami, pri čemer organ javnega zavoda nad to traso nima nadzora;
nosilec podatkov – priprava ali sredstvo, ki omogoča branje in/ali zapisovanje podatkov (disketa, CD-ROM, DVD, disk, USB-pomnilnik, kartica, trak, kaseta, papir …);
občutljivi podatki – osebni podatki (tudi občutljivi osebni podatki) po Zakonu o osebni podatkih in tajni podatki po Zakonu o tajnih podatkih ter tisti, ki jih organ javnega zavoda določi kot take;
obravnavanje podatkov – zbiranje, obdelava, prikaz, hranjenje, spreminjanje in brisanje podatkov;
ocena tveganja – ugotovitev vseh morebitnih tveganj in nevarnosti, ki lahko ogrozijo varnost in poslovanje organa javnega zavoda;
organ – organi in institucije ter njihove organizacijske enote (glej Uredbo o upravnem poslovanju);
overitelj – izdajatelj kvalificiranih digitalnih potrdil, del infrastrukture javnih ključev, ki izdaja digitalna potrdila;
relevantna zakonodaja – vsi pravni akti, ki predpisujejo pravila za neko področje (npr. tajni podatki, osebni podatki …);
penetracijski test – s strani lastnika informacijskega sistema naročen test vdora, v katerem se ugotavljajo pomanjkljivosti pri zagotavljanju informacijske varnosti;
pooblaščena oseba – posameznik ali skupina ljudi, imenovana na podlagi zakona ali s strani predstojnika organa za izvajanje določenih nalog;
prostrano omrežje – omrežje WAN. Če govorimo o državnem omrežju, je to HKOM;

protivirusni program – posebna programska oprema, ki je namenjena odkrivanju in odstranjevanju virusov in drugih zlonamernih programov;
skrbnik – pooblaščena oseba, odgovorna za upravljanje posameznega podsistema (načrtov, procesov, opreme, infrastrukture, informacijske varnosti, informacijskega sistema …);
sredstva za dostop do IS – uporabniško ime in geslo, pametne kartice, certifikati, enkratna gesla in drugi načini za avtentikacijo in avtorizacijo uporabnikov IS;
svetovni splet – internet, medmrežje;
šifriranje – preoblikovanje razumljivega besedila v nerazumljivo obliko s kriptografskimi metodami;
uporabnik – oseba, ki uporablja informacijski sistem ali napravo pri rednem delu in ima sklenjeno delovno razmerje ali je pogodbeni zunanji izvajalec;
uporabniško ime in geslo – niz znakov, s katerim se uporabnik prijavi v informacijski sistem;
upravljanje – zajem funkcij, kakršne so načrtovanje, montaža, zagotavljanje, obratovanje, administriranje in vzdrževanje sistema;
upravljavec (upravitelj) sistema – organ javnega zavoda, ki upravlja posamezni informacijski sistem ali njegov del;
varnostne kopije – so prepisi točno določenih podatkov, da se zavarujejo pred izgubo, in so navadno prepisani na optično ali magnetno sredstvo;
varovani podatek – osebni ali drug obravnavani podatek, ki ni tajen, njegovo razkritje nepoklicanim osebam pa bi lahko povzročilo škodo organu, poteku uradnih postopkov ali osebam, na katere se nanaša, zato mora njegovo obravnavanje spremljati izvajanje varnostnih ukrepov in postopkov;
varovano območje – območje, ki je pod nadzorom organa javnega zavoda, kamor spadata upravno in varnostno območje**;**
zunanji izvajalec – vsaka fizična ali pravna oseba, ki dobavi opremo ali izvaja storitve po pogodbi pri organih javne uprave.

Kršitev politike

5. člen

V informacijskem sistemu mora biti zagotovljeno zaznavanje kršitev IVPZAP in njihovo sankcioniranje po relevantni zakonodaji ali pogodbi.

6. člen

Ob morebitni kršitvi IVPZAP se lahko sprožijo ukrepi, kakršne predvideva relevantna zakonodaja. Glede na interes organa javnega zavoda se lahko uporabijo tudi drugi, nedisciplinski ukrepi. Tako imajo upravitelji pravico do takojšnje blokade in morebitne naknadne ukinitve storitve, če ugotovijo kršitev določil politike.

Veljavnost IVPZAP in zaveza vodstva

7. člen

Ukrepe IVPZAP v skladu s priporočili ministrstva, pristojnega za javno upravo, je Zgodovinski arhiv na Ptuju (ZAP) sprejel na podlagi na 80. 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) in jih je dolžan upoštevati kot krovno informacijsko varnostno politiko.

8. člen

Vodstvo Zgodovinskega arhiva na Ptuju skupaj s sistemskim administratorjem vsaj enkrat letno pregleduje izvajanje in vsebino IVPZAP ter predlaga morebitne spremembe. Izdelati mora tudi zapisnik o vodstvenem pregledu.

Skrbnik

9. člen

Skrbnik politike je vodstvo Zgodovinskega arhiva na Ptuju.

Organiziranost IVPZAP

10. člen

IVPZAP je organizirana na več ravneh. Prvo raven predstavlja krovna IVPZAP, drugo raven pa področne politike z zaokroženo celoto nekega informacijskega področja. Dokumenti tretje ravni so navodila za izvajanje nalog in skrbništva informacijskega sistema. Četrta raven so obrazci, namenjeni izvajanju nalog. Po zapisih na teh obrazcih se preverja skladnost delovanja informacijskega sistema z IVPZAP.

11. člen

Informacijska varnostna politika ZAP je objavljena na spletni strani javnega zavoda.

12. člen

Vsakdo mora upoštevati informacijsko varnostno politiko javnega zavoda Zgodovinski arhiv na Ptuju. Ko se zaposleni in pogodbeni izvajalci seznanijo z IVPZAP, podpišejo izjavo o seznanitvi z IVPZAP.

Področne politike

13. člen

Posamezna področja in v njihovem okviru postopki izvajanja IVPZAP so določeni s posebnimi varnostnimi politikami:

1. Politika fizičnega varovanja

1.1 Fizični dostop

14. člen

Za varovanje svojih prostorov skrbi ZAP sam oz. preko pooblaščenega podjetja Sintal, ki skrbi za alarmne naprave in intervencije v primeru nepooblaščenih vstopov v prostore ZAP.

15. člen

ZAP nima varnostne službe, prav tako nimam receptorja. Vstop v prostore je možen zaposlenim preko avtoriziranega dostopa (kartica/ključ). Dostop do varovanih prostorov pa je omogočen avtoriziranim osebam, ki posedujejo kartico/ključ. Vstopi se evidentirajo v evidenci kontrole pristopov.

16. člen

Vstop in gibanje obiskovalcev v ZAP je omejeno. Za nadzor dostopa se uporabljajo naslednje tehnologije: alarmni sistem, protivlomni sistem, video nadzor.

17. 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.

18. člen

Dostop uporabnikom na varovano območje je mogoč le v rednem delovnem času.

1.2 Varovanje sredstev za dostop

19. člen

Vsak zaposleni mora fizična sredstva (ključi, izkaznice, priponke, kartice itd.) in elektronska sredstva (uporabniška imena, gesla, šifrirni ključi 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.

20. člen

Morebitno krajo, izgubo ali založitev sredstva za dostop mora vsak takoj prijaviti vodstvu in sistemskemu administratorju.

Varovanje opreme

1.3 Namestitev opreme

21. člen

Vsa oprema mora biti nameščena in zaščitena tako, da so nevarnosti iz okolja in priložnosti za nepooblaščeni dostop kar najbolj odpravljene.
Raven varovanja in zaščite naj bo določena glede na občutljivost podatkov in ocenjeno tveganja izgube ali poškodovanja podatkov.

1.4 Protipožarno varovanje

22. 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.

1.5 Zaščita ožičenja

23. 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. Pri vsaki nadgradnji ali spremembi omrežja ali vanj vključenih naprav mora biti preverjena varnost ožičenja.

24. člen

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

25. 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.

26. člen

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

1.6 Okvare in poškodbe opreme

27. člen

Uporabniki morajo vsako okvaro in namerno ali nenamerno poškodbo opreme sporočiti sistemskemu administratorju , ki mora ukrepati v skladu s predpisanimi postopki.

2. Politika primerne rabe informacijskih sistemov in zaščite občutljivih podatkov

2.1 Uporaba opreme informacijske tehnologije

28. člen

Informacijska oprema v lasti Zgodovinskega arhiva na Ptuju je namenjena opravljanju oziroma potrebam dela v javnem zavodu. Uporaba v zasebne namene ni dovoljena razen za nujne zadeve in v manjšem obsegu, ki ne moti delovnega procesa in varnosti (zaupnost, celovitost in razpoložljivost) informacijskega sistema, ali če jo pisno odobri predstojnik organa ali institucije javnega zavoda.

29. člen

Uporabniki morajo z informacijsko opremo javnega zavoda ravnati kakor dober gospodar, po priporočilih proizvajalca in skrbnika sistema. Posege vanjo lahko opravljajo samo za to pooblaščene osebe.
Za odtujitev in poškodbe opreme je odgovoren uporabnik. Posebno skrbno mora ravnati s prenosno opremo.

30. člen

Uporabniki 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.

2.2 Zlonamerna programska oprema

31. 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.

Uporabniki:

- morajo, če sumijo, da na informacijskem sistemu deluje zlonamerna programska oprema, takoj nehati delati z njim, obvestiti pristojno osebo in upoštevati njena 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 upravljavca in upoštevati njegova navodila;

2.3 Informacijski sistemi

32. člen

Informacijski sistemi, ki obravnavajo občutljive podatke, morajo biti nadzorovani.

33. člen

Uporaba zasebne opreme v informacijskem sistemu javnega zavoda ni dovoljena.

2.4 Upravljanje izmenljivih nosilcev podatkov

34. člen

Zagotovljena morata biti ustrezno varovanje in zaščita pri upravljanju izmenljivih nosilcev podatkov.

35. člen

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

36. člen

Nosilci podatkov, ki niso last javnega zavoda se ne smejo uporabljati. Preden se uporabi vsebina izmenljivega nosilca podatkov, ki je v lasti javnega zavoda, se mora vselej preveriti njegova morebitna okuženost z zlonamerno programsko opremo.

37. člen

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

2.5 Dostop do informacijskih sistemov

38. člen

Za dostop informacijskega sistema ZAP mora biti vzpostavljen postopek dodelitve, sprememb in prenehanja dostopnih pravic.

39. člen

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

40. člen

Na podlagi potreb poslovnega procesa se odobri dostop do informacijskega sistema v obsegu, ki je potreben za opravljanje delovnih nalog. Obseg dostopa in pravice se izvedejo na podlagi zahtevka, ki ga vodja poda sistemskemu administratorju, le-ta pa poskrbi za njegovo realizacijo.

41. člen

Dostop do informacijskih sistemov javnega zavoda mora biti mogoč le na podlagi ustrezne avtentikacije, minimalno z uporabo uporabniškega imena in gesla.

42. člen

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

43. 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 sistemskemu administratorju.

44. 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.

45. člen

Pravico dostopa do informacijskega sistema ali omrežja lahko pridobijo uporabniki 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.

46. člen

Uporabniške in administratorske pravice dostopa do informacijskih sistemov so ločene.

47. 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.

2.6 Načelo čiste mize

48. člen

Uporabniki 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 uporabnikov ni v prostoru, morajo biti nosilci podatkov varno shranjeni. 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.

2.7 Načelo praznega zaslona

49. 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.

2.8 Oddaljeni dostop

50. člen

Oddaljeni dostop do informacijskega sistema je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer za tiste uporabnike, 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.

51. 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 javne uprave šifrira.

2.9 Dostop do svetovnega spleta in storitev v svetovnem spletu

52. člen

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

53. člen

Zaposleni v javnem zavodu 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 javnega zavoda (IP naslov).

54. člen

Na podlagi ocene tveganja je mogoče omejevati dostop do različnih tipov vsebin (Stream media, P2P, Flash media…) zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev etičnih in moralnih norm.

55. člen

Pošiljanje službenih elektronskih naslovov na zunanje spletne strežnike ni dovoljeno, razen če je povezano s poslovnim procesom ZAP.

56. člen

V omrežju javnega zavoda ZAP 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 upravljavci posredujejo le na obrazloženo zahtevo organa, ki na podlagi zakonskih pooblastil obravnava domnevno nezakonita dejanja.
Drugačna obdelava podatkov iz prvega stavka ni dovoljena. Rok hrambe teh sintetiziranih podatkov je tri mesece, nato se podatki uničijo ali anonimizirajo. Anonimizirani podatki se lahko uporabljajo za upravljanje sistema.

57. člen

V omrežju javnega zavoda ZAP se na zahtevo vodstva lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja za načrtovanje in varovanje informacijskega sistema.

2.10 Uporaba elektronske pošte

58. člen

Zaposleni v javnem zavodu ZAP kot orodje za komunikacijo z državljani, strankami, zaposlenimi in zunanjimi izvajalci uporabljajo tudi elektronsko pošto. Pri tem se morajo držati ne le etičnih in moralnih norm, temveč tudi bontona.
Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje organa, v katerem je pošiljatelj zaposlen.

59. člen

Sistem elektronske pošte se praviloma uporablja samo v službene namene. Uporaba v druge namene je dopustna le izjemoma, če ne moti delovnega procesa in varnosti (zaupnost, celovitost in razpoložljivost) informacijskega sistema.

60. 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.

61. člen

Uporabniki svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove.
Prav tako se zaposleni ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi javnega zavoda, razen če to ni povezano s potrebami delovnega mesta.

62. 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 sistemskega administratorja v arhivu.

63. člen

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

64. 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.

2.11 Pravice nad podatki elektronske pošte

65. člen

Vse pravice na sistemu elektronske pošte in vseh elektronskih sporočilih, ki niso zasebna, pripadajo organu javnega zavoda - ZAP. Uporabniki se morajo zavedati, da se elektronska sporočila v sistemu elektronske pošte varnostno shranjujejo.

66. člen

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

67. 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.

68. 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 pristojnega državnega organa ali v izjemnih primerih posebnega pisnega pooblastila predstojnika organa javnega zavoda. Pri tem se morajo upoštevati določila relevantne zakonodaje in vsa pravila, ki v takšnih primerih veljajo za ravnanje z gesli.

69. člen

Elektronska sporočila, ki prihajajo na enotne namenske elektronske poštne naslove (npr. tajništvo, čitalnica, pisarna za izdajo dokumentov), odpirajo za to pooblaščene ali dodeljene osebe, ki v času odsotnosti nadomeščajo zaposlenega.

2.12 Privzete nastavitve predala

70. člen

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

2.13 Velikost elektronskih sporočil

71. člen

Največja velikost sporočil pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena. Omejitev določa sistemski administrator elektronske pošte. Če je omejitev presežena (cca 10 MB) se sporočilo samodejno zavrne, pošiljatelj pa dobi obvestilo o prevelikem obsegu.

72. člen

Če uporabnik 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.

73. člen

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

74. člen

Uporabnik 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.

75. člen

Pri ravnanju z občutljivimi podatki je treba dosledno upoštevati zakonodajo.

2.14 Šifriranje in podpisovanje elektronskih sporočil

76. člen

Šifriranje in podpisovanje elektronskih sporočil se lahko izvaja samo z uporabo odobrenih metod v organu javnega zavoda.

2.15 Brisanje elektronskih sporočil

77. člen

Pri shranjevanju elektronskih sporočil morajo uporabniki upoštevati načelo racionalnosti in se izogibati hranjenju dokumentov v multimedijskih podatkovnih formatih, ki zavzamejo veliko prostora (filmi, slike visoke resolucije, zvočni zapisi).
Elektronska sporočila, ki so zasebne narave, morajo uporabniki brisati sproti.

78. člen

Nezaželeno pošto ima upravitelj dolžnost brisati.

2.16 Posebna pooblastila

79. člen

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

80. člen

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

2.17 Dostop do podatkov

81. 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.

82. člen

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

83. člen

Vse zbirke občutljivih sistemskih podatkov (gesla, videonadzor,sistemski dnevniki) morajo imeti vzpostavljene ustrezne dnevnike vpogledov, v katerih je zabeleženo: kdo, kdaj in zakaj je opravil vpogled, skladno z relevantno zakonodajo. Vodeni morajo biti tudi vsi servisni in vzdrževalni posegi na strežniku, bazi, aplikaciji ali storitvi.

84. 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).

85. člen

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

86. 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 ni dovoljeno.

87. 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.

88. 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.

89. člen

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

3. Politika nabave opreme in storitev pri zunanjih izvajalcih

3.1 Priprava javnega naročila

90. člen

Pri pripravi specifikacij javnega naročila za nabavo gradnikov ali vzdrževanje informacijskih sistemov je treba predvideti in opredeliti varnostne elemente, ki bodo izpolnjevali zahteve informacijske varnostne politike javne uprave in relevantne zakonodaje.

91. člen

Po potrebi mora izvajalec javnega naročila občutljivo dokumentacijo in podatke pred objavo ustrezno klasificirati. Pri tem je treba upoštevati določila relevantne zakonodaje.

92. člen

Pri pripravi javnega naročila je treba določiti tehnične, ekonomske in kadrovske pogoje ter merila za izbiro ponudnikov z vidika zagotavljanja ciljev varnostne politike.

93. člen

Izvajalec mora biti ustrezno varnostno preverjen in imeti ustrezno izobrazbo (primerno ravni storitve). O spremembah redno obvešča naročnika.

3.2 Varnostni elementi v pogodbi

94. člen

V pogodbah morajo biti določeni predmet in obseg storitve, merila, obveznosti in s tem povezane posledice, ki vplivajo na kakovostno izvedbo pogodbenih obveznosti glede varnostne politike.
Pogodbe z zunanjimi izvajalci morajo vsebovati določila o seznanjenosti z IVPZAP in sprejemanju te politike ter zavezanost k varovanju podatkov, kjer je to potrebno. Zunanji izvajalci, podizvajalci in njihovi zaposleni, ki bodo izvajali dela po pogodbi, morajo pred sklenitvijo pogodbe podpisati izjave o seznanitvi z IVPZAP in sprejemanju te politike.
Za veljavne pogodbe, sklenjene pred uveljavitvijo IVPZAP, je treba z izvajalci skleniti ustrezne dodatke k pogodbam in podpisati izjave, kjer je to smiselno in izvedljivo.

95. člen

V pogodbi ali drugem navodilu morata biti, če je to potrebno, določena način fizičnega dostopa do informacijskega premoženja javnega zavoda in način prijave v informacijski sistem javnega zavoda.
Podeljene pravice dostopa do informacijskega premoženja javnega zavoda morajo biti vezane na konkretno fizično osebo in dokumentirane. Spremembe, ki vplivajo na
podeljene dostopne pravice, mora zunanji izvajalec redno sporočati in uskladiti z naročnikom.
Dostopi in posegi zunanjih izvajalcev v informacijske sisteme javnega zavoda morajo biti beleženi.

96. člen

V pogodbah, po katerih zunanji izvajalci obdelujejo občutljive podatke, mora biti natančno opredeljeno, kateri podatki in kako se lahko obdelujejo.
V pogodbah morajo biti opredeljeni način, vrsta in pogostnost nadzora nad zunanjimi izvajalci, ki ga v zvezi z informacijsko varnostjo redno opravlja naročnik ali njegov pooblaščenec ali ustrezen certifikacijski organ.

97. člen

V pogodbi morajo biti določeni postopki in sankcije za kršitve IVPZAP.

98. člen

V pogodbah ali izvedbenih navodilih, ki vključujejo vzdrževanje informacijskih sistemov, morajo biti opredeljeni načini in postopki za zagotavljanje neprekinjenega poslovanja.

99. člen

Pogodba o zagotavljanju storitev vsebuje tudi določila za minimizacijo časa izpada storitve.

3.3 Izvajanje pogodbe

100. člen

Za izboljšanje ravni storitve se morata naročnik in izvajalec dogovoriti o načinu spremembe postopkov. Naročnik mora pregledovati postopke ob spremembah ali najmanj enkrat na leto. Vse spremembe morajo biti dogovorjene in usklajene med naročnikom in izvajalcem.

Nadzor

101. člen

Naročnik in izvajalec določita skrbnike pogodb, ki skupaj z upravljavcem sproti preverjajo ustreznost v pogodbi opredeljene storitve.
Zunanji izvajalec mora skrbniku pogodbe redno dostavljati poročila o njenem izvajanju.

102. člen

Informacijske rešitve ali deli informacijskih rešitev, ki jih je zunanji izvajalec namensko razvil za organ javnega zavoda in bi lahko ogrozili varnost informacijskega sistema organa, postanejo s prevzemom last organa. Zunanji izvajalec teh rešitev ne sme dati naročnikom zunaj javnega zavoda.

4. Politika razvoja in vzdrževanja informacijskih sistemov in obvladovanja sprememb

4.1 Načrtovanje

103. 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.

104. člen

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

105. 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.

4.2 Razvojno okolje

106. člen

Razvoj informacijskih storitev se mora izvajati v razvojnem okolju tako, da ne vpliva na produkcijsko okolje. Razvojno okolje je dostopno le skupini razvijalcev in naročniku ter je lahko nameščeno tudi pri zunanjih razvijalcih.

107. člen

Zagotovljeni morajo biti vsi potrebni varnostni mehanizmi, ki nepooblaščenim osebam onemogočajo dostop do razvojnega okolja in dokumentacije.

108. člen

Pri razvoju programske opreme mora biti vzpostavljen ustrezen sistem nadzora različic dokumentacije in programske kode. Iz oznake različic mora biti določljiv kronološki vrstni red njihovega nastajanja.

109. člen

Uporaba produkcijskih podatkov v razvojnem okolju ni dovoljena.

4.3 Testno okolje

110. člen

Testno okolje mora biti v upravljanju in pod nadzorom organa javnega zavoda.

111. člen

Nameščanje in spreminjanje strojne opreme, aplikacij in zbirk podatkov mora naročati, odobriti in nadzirati organ javnega zavoda.
Zunanji izvajalci projekta lahko sodelujejo pri postopku namestitve, vendar ga ne smejo izvajati brez nadzora. Vse spremembe in postopki morajo biti dokumentirani in različice obvladane.

112. člen

Naročnik mora preveriti in potrditi funkcionalnost, varnost in zmogljivost same aplikacije ali strojne opreme, aplikacije ali strojne opreme v povezavi z informacijskim sistemom in vpliv na celoten informacijski sistem.

113. člen

Testno okolje mora biti ločeno od produkcijskega, tako da vpliv na slednjega ni mogoč.
Testno okolje mora biti čim bolj podobno produkcijskemu in za oba veljajo enake varnostne zahteve.
Uporaba produkcijskih podatkov v testnem okolju ni dovoljena.

4.4 Izobraževalno okolje

114. člen

Okolje, namenjeno izobraževanju uporabnikov, mora biti ločeno od drugih okolij in vsebuje lahko le izmišljene testne primere, ki omogočajo izvedbo predstavitve funkcionalnosti. Biti mora dostopno le v izobraževalne namene.

4.5 Produkcija

115. člen

O pogojih za izvedbo sprememb v produkcijskem okolju se dogovorita naročnik in skrbnik informacijskega sistema. Spremembe, ki zahtevajo prekinitev v delovanju informacijskega sistema, morajo biti načrtovane in vnaprej napovedane. Vsako izvedeno spremembo je treba evidentirati.

116. člen

Vzpostavljen in dokumentiran mora biti postopek prenosa programske in/ali strojne opreme v produkcijsko okolje za vsak informacijski sistem. Postopek mora vključevati uporabniške in zmogljivostne teste z dokazili o izpolnjevanju naročnikovih zahtev.
Priloženo mora biti potrdilo, da spremembe ne vplivajo na delovanje drugih informacijskih sistemov in da so v informacijski sistem vgrajeni vsi zahtevani varnostni elementi. Postopek prenosa mora biti pod nadzorom.

117. člen

Pred prenosom nove aplikacije, njene nove različice ali popravka aplikacije v produkcijsko okolje morajo biti opravljeni in dokumentirani vsi predhodni razvojni in testni postopki. Izdelana morajo biti navodila za namestitev aplikacije, ki vsebujejo opis postopkov ter potrebnega časa za namestitev in varnostno poročilo. Upoštevati je treba tudi sistemske zahteve, ki so bile ugotovljene v razvojnem ali testnem okolju.

118. člen

Vzpostavljen mora biti postopek preverjanja programske kode zaradi preprečitve znanih varnostnih pomanjkljivosti v programski kodi.

119. člen

Vzpostavljeni in dokumentirani morajo biti postopki, ki po kakršni koli spremembi informacijskega sistema v produkcijskem okolju omogočajo povrnitev v stanje pred spremembo.

4.6 Pravice dostopa

120. člen

Zunanji izvajalci smejo imeti dostop do produkcijskega okolja izključno le pod ustreznim nadzorom naročnika.

121. člen

Dostop do produkcijskih podatkov v informacijskih sistemih javnega zavoda je zunanjim izvajalcem prepovedan. Izjemoma jim je lahko dovoljen pod nadzorom naročnika in na podlagi njegovega posebnega pisnega dovoljenja, ki velja le za posamezen primer in v omejenem obsegu.

122. člen

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

123. člen

Izvedeno mora biti beleženje uspešnih in neuspešnih prijav v informacijske sisteme ter ustrezno zaklepanje računov ob neuspešni prijavi.

124. člen

Uporabniške seje morajo biti časovno omejene. Vzpostavljen mora biti mehanizem, ki samodejno prekine neaktivne seje.

5. Politika upravljanja informacijskega sistema

5.1 Upravljanje produkcijskega okolja

125. člen

Produkcijska okolja informacijskih sistemov in omrežja javnega zavoda morajo biti pod nadzorom in v upravljanju organov javnega zavoda. Storitve upravljanja produkcijskega okolja ali omrežja javnega zavoda lahko izvajajo zunanji izvajalci, ki imajo sklenjene pogodbe o dobavi storitev.

126. člen

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

127. člen

Za omrežje in njegovo varnost je na vsakem organu zadolžen skrbnik omrežja. Ta stalno preverja nespremenljivost omrežja in njegovo skladnost z dokumentacijo. Preverja fizične in logične nastavitve njegovih gradnikov in omrežja samega ob spremembah ali najmanj enkrat na leto.

5.2 Dokumentirani delovni postopki

128. člen

Postopki, ki so povezani z delovanjem informacijskega sistema, morajo biti dokumentirani. Za to mora poskrbeti upravljavec. Ob spremembah postopkov je treba posodobiti tudi dokumentacijo. Ta mora biti pregledana vsaj enkrat na leto in biti na voljo na kraju uporabe.

5.3 Upravljanje sprememb v produkcijskem okolju in omrežju

129. člen

Ob spremembah v informacijskem sistemu mora biti zagotovljena njegova zaupnost, celovitost in čim večja razpoložljivost. Pred vsako spremembo v njem mora biti izdelan načrt povrnitve v predhodno stanje.

130. člen

O spremembah v informacijskem sistemu, ki bi lahko povzročile spremembe pri rednem delu uporabnikov sistema, so ti ustrezno obveščeni.

5.4 Ločevanje nalog

131. člen

Upravljanje informacijskih sistemov in omrežij mora biti razdeljeno na več nalog, ki jih, če je to mogoče, opravljajo različne osebe. Izvajanje nalog je treba ustrezno nadzorovati.

5.5 Zaščita pred zlonamerno in prenosno kodo

132. člen

Omrežja javnega zavoda morajo imeti vgrajene mehanizme, ki omogočajo zaznavanje in preprečevanje zlonamerne programske opreme že na mrežni ravni.
Mehanizme za zaznavanje in preprečevanje zlonamerne programske opreme morajo imeti tudi zasebna omrežja, ki se priklapljajo v prostrano omrežje javnega zavoda.

5.6 Nadzor dostopa do omrežja

133. člen

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

5.7 Ločevanje v omrežjih

134. člen

Omrežja, ki imajo različne politike dostopa, so med seboj ločena. Če nastane potreba po povezovanju, je treba spoštovati politiko povezovanja med omrežji, ki jo določijo njihovi lastniki. Pri tem morajo zagotoviti izpolnjevanje relevantne zakonodaje in varnostnih zahtev v vseh omrežjih.

5.8 Upravljanje omrežnega usmerjanja

135. člen

Usmerjanje podatkovnega prometa po prenosnih poteh v omrežjih je nadzorovano in upravljano za zagotavljanje kakovosti storitev. Spremembe se izvajajo po postopku upravljanja sprememb.

5.9 Upravljanje incidentov pri varovanju informacij

136. člen

Upravljavci morajo zagotoviti, da se dejavnosti in dogodki v informacijskih sistemih beležijo.
Na podlagi ugotovljenih dogodkov morajo izvajati ustrezne ukrepe.

137. 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.

138. člen

Voditi je treba zapise o incidentih.

5.10 Dnevniški zapisi

139. člen

Redno se izdelujejo dnevniški zapisi o spremembah in posegih v informacijskem sistemu. Obseg podatkov v dnevniških zapisih in rok hrambe morata biti sorazmerna z namenom beleženja in morata upoštevati določbe relevantne zakonodaje.

140. člen

Zagotovljeni morata biti celovitost in nespremenljivost dnevniških zapisov, ki jih pregleduje upravljavec za potrebe upravljanja informacijskega sistema ali omrežja. Dostop do dnevniških zapisov imajo za to pooblaščene osebe upravljavca in druge osebe na podlagi zakona. Postopki in ukrepi morajo onemogočati možnost spreminjanja ali nepooblaščenega
izklopa revizijskih sledi (podatkov v dnevnikih).

5.11 Obdelava podatkov v dnevniških zapisih

141. člen

Dnevniški zapisi, ki vsebujejo občutljive podatke, se hranijo, obdelujejo in pošiljajo skladno z določbami zakona, vsak dostop do takšnih zapisov ali druga oblika obdelave podatkov v njih pa mora biti zabeležena. Vsaka izjema mora biti pisno obrazložena z oceno tveganja.

5.12 Ravnanje na podlagi ugotovitev iz dnevniških zapisov

142. člen

Na podlagi sporočil posameznih informacijskih sistemov ali posameznih mrežnih naprav se izločajo dnevniški zapisi, ki nakazujejo napako na napravi ali nedovoljeno dejavnost. Upravljavec take zapise obravnava kot incident in se odzove primerno njegovi ravni ter poskrbi za ustrezno obveščanje. Če je incident tehnične narave, takoj ustrezno ukrepa, sicer počaka na navodila skrbnika informacijskega sistema.

143. člen

Neodobrene mrežne opreme ni dovoljeno priklapljati v omrežje.

5.13 Kriptografske rešitve

144. člen

Kriptografske kontrole so uvedene na vseh mrežnih komunikacijskih napravah, ki povezujejo med seboj različne lokacije (promet po nezavarovanem območju – fizično ali logično).

145. člen

Kriptografski ključi se ustvarijo in hranijo v za to prirejenih prostorih. Obnova ključev je samodejna, kjer je to mogoče.

146. člen

Kriptografija se uporabi pri povezovanju sistemov, za katere veljajo stopnje tajnosti ali ki obravnavajo občutljive podatke. Dovoljeno je uporabljati le tiste kriptografske rešitve, ki jih odobri za to pristojen organ oziroma imajo izdano potrdilo o varnostni ustreznosti.

5.14 Raba virov

147. člen

Raba vseh virov, ki so vključeni v delovanje produkcijskega okolja, mora biti spremljana in upravljana tako, da omogoča zahtevano kakovost storitve. Vodstvo mora poskrbeti, da so viri za zagotavljanje nemotenega delovanja skladni z načrtom neprekinjenega poslovanja.

5.15 Oskrba z električno energijo

148. člen

Ključna oprema in pomožne informacijske naprave morajo biti priključene na sistem neprekinjenega napajanja (UPS) in rezervni generator.

5.16 Klimatski pogoji

149. člen

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

5.17 Varnostne kopije

150. 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.

151. člen

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

5.18 Upravljanje neprekinjenega poslovanja

152. člen

Poslovni procesi v javnem zavodu, ki so podprti z informacijskimi sistemi, morajo imeti 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.

153. člen

Skrbniki načrtov neprekinjenega poslovanja so lastniki procesov.

154. člen

Načrti neprekinjenega poslovanja morajo biti redno (najmanj enkrat na leto ali ob spremembi) preverjani v praksi in sproti dopolnjevani.
Skrbniki infrastrukture, ki zagotavlja delovanje informacijskih sistemov, morajo skupaj z upravljavci in lastniki procesov ter uporabniki redno izvajati simulacije izpadov in preverjati pravilno vzpostavitev ponovnega delovanja.
O preizkušanju načrtov neprekinjenega poslovanja je treba voditi zapise in o izsledkih obveščati vodstvo.

155. člen

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

156. člen

Skrbniki informacijskih sistemov morajo redno vzdrževati produkcijsko okolje in omogočati njegovo neprekinjeno delovanje. Vodstvo in skrbniki pa morajo skupaj načrtovati razvoj infrastrukture in zagotavljati vire za njeno nemoteno delovanje.

5.19 Vzdrževanje opreme

157. člen

Za vso opremo mora biti zagotovljeno vzdrževanje, ki ga lahko opravlja strokovna služba ali pooblaščeni izvajalci. Če vzdrževanje opravijo zunanji izvajalci, morajo biti podatki zavarovani tako, da je onemogočen nepooblaščeni dostop do njih.

158. člen

Za vsak kos opreme, ki zapusti organ javnega zavoda zaradi vzdrževanja, je treba imeti prevzemni dokument.

5.20 Vzdrževalna dela

159. 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.

6. Prehodne in končne določbe

160. člen

IVPZAP začne veljati naslednji dan po sprejetju Sveta zavoda ZAP in objavi na spletni strani Zgodovinskega arhiva na Ptuju.

Ptuj, dne 08.08.2016

Katja ZUPANIČ
DIREKTORICA ZAP