Na podlagi Družbene pogodbe o ustanovitvi JAVNEGA HOLDINGA Ljubljana, d.o.o., družba za izvajanje strokovnih in razvojnih nalog na področju gospodarskih javnih služb (notarsko potrdilo opr. št.: SV 1687/13 z dne 17.09.2013 – prečiščeno besedilo) sprejemam naslednjo

KROVNO INFORMACIJSKO VARNOSTNO POLITIKO JAVNEGA HOLDINGA LJUBLJANA

Kazalo vsebine

Namen in cilji ... 4
Uporabljeni izrazi ... 5
Kršitev politike ... 7
Veljavnost Informacijske varnostne politike in zaveza poslovodje ... 7
Skrbnik ... 8
Ocena tveganja ... 8
Organiziranost Informacijske varnostne politike ... 8
Področne politike ... 9
1. Politika fizičnega in tehničnega varovanja ... 9
Fizični dostop ... 9
Varovanje sredstev za dostop ... 10
Varovanje opreme ... 10
Namestitev opreme ... 10
Protipožarno varovanje ... 10
Zaščita ožičenja ... 11
Okvare in poškodbe opreme ... 11
2. Politika primerne rabe informacijskega sistema in zaščite občutljivih podatkov ... 11
Uporaba opreme informacijske tehnologije ... 11
Zlonamerna programska oprema ... 12
Informacijski sistem ... 12
Upravljanje izmenljivih nosilcev podatkov ... 13
Dostop do informacijskega sistema ... 13

Načelo čiste mize ... 14
Načelo praznega zaslona ... 15
Oddaljeni dostop ... 15
Dostop do svetovnega spleta in storitev v svetovnem spletu ... 15
Uporaba elektronske pošte ... 16
Pravice nad podatki elektronske pošte ... 17
Privzete nastavitve predala ... 18
Velikost elektronskih sporočil ... 18
Šifriranje in podpisovanje elektronskih sporočil ... 19
Brisanje elektronskih sporočil ... 19
Posebna pooblastila ... 19
Dostop do podatkov ... 20
3. Politika nabave opreme in storitev pri zunanjih izvajalcih ... 21
Priprava javnega naročila ... 21
Varnostni elementi v pogodbi ... 21
Izvajanje pogodbe ... 22
Nadzor ... 22
4. Politika razvoja in vzdrževanja informacijskega sistema in obvladovanja sprememb ... 23
Načrtovanje ... 23
Razvojno okolje ... 23
Testno okolje ... 24
Izobraževalno okolje ... 24
Produkcija ... 24
Pravice dostopa ... 25
5. Politika upravljanja informacijskega sistema ... 26
Upravljanje produkcijskega okolja ... 26
Dokumentirani delovni postopki ... 26
Upravljanje sprememb v produkcijskem okolju in omrežju ... 26
Ločevanje nalog ... 27
Zaščita pred zlonamerno in prenosno kodo ... 27
Časovna uskladitev ... 27
Nadzor dostopa do omrežja ... 27
Ločevanje v omrežjih ... 27

Upravljanje omrežnega usmerjanja 27
Upravljanje incidentov pri varovanju informacij 27
Dnevniški zapisi 28
Obdelava podatkov v dnevniških zapisih 28
Ravnanje na podlagi ugotovitev iz dnevniških zapisov 28
Kriptografske rešitve 29
Raba virov 29
Oskrba z električno energijo 29
Klimatski pogoji 29
Varnostne kopije 29
Upravljanje neprekinjenega poslovanja 30
Vzdrževanje opreme 31
Vzdrževalna dela 31
Prehodne in končne določbe 31

Namen in cilji

1. člen

Informacijska varnostna politika (dalje: IVP) JAVNEGA HOLDINGA Ljubljana, d.o.o. (dalje: JHL) izraža politiko, s katero želi JHL zaščititi informacijsko premoženje, ki ga upravlja.

IVP JHL služi kot neposreden vir pravil in navodil za učinkovito in varno uporabo informacijskega sistema in za varovanje podatkov - za JHL, povezana javna podjetja in druga podjetja, ki uporabljajo informacijsko infrastrukturo in storitve JHL (dalje: družbe uporabnice).

2. člen

Namen IVP JHL je postaviti osnovna varnostna izhodišča za zaščito informacijskega sistema in podatkov oziroma informacij pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi in omejevanje škode s preprečevanjem in zmanjševanjem vpliva incidentov.

Izvajanje IVP JHL 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 IVP JHL se vzpostavlja stalen postopek zagotavljanja in vzdrževanja informacijske varnosti in upravljanje s tveganji ter s tem doseganje naslednjih temeljnih ciljev:

- zavarovanje podatkov/informacij pred nepooblaščenim dostopom, obdelavo in razkritjem,
- zagotavljanje in 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,
- zaznavanje, beleženje in raziskovanje kršitev IVP JHL ter ukrepanje pri ugotovljenih kršitvah oziroma v primerih utemeljenega suma kršitev,
- zagotavljanje in preverjanje skladnosti z zakonodajo,
- upoštevanje priporočil glede standardov informacijske varnosti.

Uporabljeni izrazi

4. člen

V tem aktu imajo uporabljeni izrazi naslednji pomen:

- digitalno potrdilo – potrdilo, ki vsebuje podatke o identiteti imetnika, izdajatelja in imetnikov javni ključ, s katerim se overi elektronski podpis;
- dnevnik obiskovalcev – evidenca v elektronski ali pisni obliki s podatki o obiskovalcu, namenu in času obiska;
- 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 (dalje: IS) – celoten skupek opreme (komunikacijske in informacijske) in postopkov za obravnavanje podatkov družbe;
- informacijski varnostni dogodek – vsak dogodek, ki lahko vpliva na varnost podatkov v IS ali na delovanje IS;
- infrastruktura – energetski in komunikacijski vodi, generatorji, klimatske naprave, sistemi neprekinjenega napajanja (sistemi UPS), sistemi za gašenje, prostori ...;
- internet - javno dostopno omrežje;
- intranet - lokalno omrežje znotraj družbe, ki ni dostopno javnosti;
- 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 družbe;

- lokalno omrežje (LAN) – računalniško omrežje z aktivnimi in pasivnimi elementi, ki omogoča povezljivost ter pretok podatkov med terminalsko opremo in viri v družbi;
- 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 družba 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) v skladu s predpisi, ki urejajo varstvo osebnih in tajnih podatkov ter tistimi, ki jih posamezna družba uporabnica 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 družbe;
- družbe uporabnice – JHL ter povezana javna podjetja in druga podjetja, ki uporabljajo IS in storitve JHL;
- overitelj – izdajatelj kvalificiranih digitalnih potrdil, del infrastrukture javnih ključev, ki izdaja digitalna potrdila;
- penetracijski test – s strani družbe uporabnice IS naročen test vdora, v katerem se ugotavljajo pomanjkljivosti pri zagotavljanju informacijske varnosti;
- pooblaščena oseba – posameznik ali skupina ljudi, imenovana na podlagi internega akta s strani posamezne družbe uporabnice za izvajanje določenih nalog;
- prostrano omrežje – omrežje WAN. Celotno omrežje, ki ga upravlja notranja organizacijska enota JHL, pristojna za informatiko;
- 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, IS ...);
- 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 IS ali napravo pri rednem delu in ima sklenjeno delovno razmerje ali je pogodbeni zunanji izvajalec;

- uporabniško ime in geslo – ime je niz znakov, s katerim se uporabnik prijavi v IS. Geslo je posebna šifra, ki se praviloma poleg uporabniškega imena zahteva za dostop do zaklenjenega programa ali naprave;

- upravljanje – zajem funkcij, kakršne so načrtovanje, montaža, zagotavljanje, obratovanje, administriranje in vzdrževanje sistema;

- upravljavec (upravitelj) IS – notranja organizacijska enota JHL, pristojna za informatiko, ki upravlja posamezni IS 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 družbam uporabnicam oziroma posamezni družbi uporabnici, izvajanju poslovnih procesov ali osebam, na katere se nanaša, zato mora njegovo obravnavanje spremljati izvajanje varnostnih ukrepov in postopkov;

- varovano območje – območje, ki je pod nadzorom posamezne družbe uporabnice, kamor spadata upravno in varnostno območje, kakor je določeno v predpisih, ki urejajo varstvo osebnih in tajnih podatkov;

- zunanji izvajalec – vsaka fizična ali pravna oseba, ki dobavi opremo ali izvaja storitve po pogodbi pri družbah uporabnicah oziroma posamezni družbi uporabnici.

V tem aktu uporabljeni izrazi, ki se nanašajo na osebe in so zapisani v moški slovnični obliki, so uporabljeni kot nevtralni za ženski in moški spol.

Kršitev politike

5. člen

V IS mora biti zagotovljeno zaznavanje, beleženje in raziskovanje kršitev IVP JHL in ukrepanje v primeru ugotovljenih kršitev oziroma v primeru utemeljenega suma kršitev skladno s predpisi, internimi akti JHL ali določili pogodbe.

Upravitelj IS v primeru ugotovljenih kršitev oziroma v primeru utemeljenega suma kršitev izvede takojšnjo blokado in ostale potrebne ukrepe za omejitev škode s preprečevanjem in zmanjševanjem vpliva incidentov, tudi z ukinitvijo storitve.

Veljavnost Informacijske varnostne politike in zaveza poslovodje

6. člen

IVP JHL sprejme poslovodja JHL, vse ostale družbe uporabnice pa so jo, po pristopu k veljavnosti IVP JHL, ki ga pisno podajo poslovodje teh podjetij, dolžne upoštevati kot krovno IVP.

Poslovodja JHL se zaveže, da bo s tem dokumentom oblikovana IVP JHL skladna z mednarodnimi standardi, ki vsebujejo zahteve, povezane s Sistemom vodenja varovanja informacij.

7. člen

Raven izvajanja IVP JHL pregleduje poslovodja JHL vsaj enkrat na leto na podlagi poročila o pregledu izvajanja IVP JHL skladno z mednarodnimi standardi, ki ga pripravi upravitelj IS.

Skrbnik

8. člen

Skrbnik IVP JHL je vodja notranje organizacijske enote JHL, pristojne za informatiko. Politiko najmanj enkrat na leto pregleduje in predlaga spremembe delovna skupina za informacijsko varnost.

Delovno skupino za informacijsko varnost imenuje poslovodja JHL. Člane delovne skupine predlagajo poslovodje družb uporabnic.

Ocena tveganja

9. člen

Metodologijo za izdelavo ocene tveganja, ki mora biti skladna z mednarodnimi standardi, na predlog delovne skupine za informacijsko varnost potrdijo poslovodje družb uporabnic.

Organiziranost Informacijske varnostne politike

10. člen

IVP JHLje organizirana na več ravneh.

Prva raven je krovna IVP JHL, druga raven so področne politike iz 13. člena te IVP JHL.

Tretja raven so interni akti za izvajanje nalog in skrbništva IS. Pripravljajo jih posamezne družbe uporabnice. Za enake oziroma za IS in storitve, ki se uporabljajo v več posameznih družbah uporabnicah, se akti pripravijo skupaj z delovno skupino za informacijsko varnost.

Četrta raven so obrazci, namenjeni izvajanju nalog. Po zapisih na teh dokumentih se preverja skladnost delovanja IS z IVP JHL.

11. člen

IVP JHL je objavljena na intranetnem spletnem naslovu posamezne družbe uporabnice oziroma na običajen način, kot se objavljajo interni akti v posamezni družbi uporabnici.

12. člen

Vsakdo, ki ima dostop do IS mora upoštevati IVP JHL in vse področne politike na vseh ravneh, ki so vezane na njegove delovne naloge ali pogodbene obveznosti.

13. člen

Posamezna področja in v njihovem okviru postopki izvajanja IVP JHL so določeni s posebnimi področnimi varnostnimi politikami:

- politika fizičnega varovanja,
- politika primerne rabe informacijskega sistema in zaščite občutljivih podatkov,
- politika nabave opreme in storitev pri zunanjih izvajalcih,
- politika razvoja in vzdrževanja informacijskega sistem in obvladovanja sprememb in
- politika upravljanja informacijskega sistema.

1. Politika fizičnega in tehničnega varovanja

Fizični dostop

14. člen

Vsaka posamezna družba uporabnica mora poskrbeti za ustrezno fizično ali tehnično varovanje svojih prostorov. Za to poskrbi z varnostno službo, ki opravlja naloge skladno s predpisi in področno politiko fizičnega in tehničnega varovanja ter načrti fizičnega in tehničnega varovanja.

15. člen

Vsaka posamezna družba uporabnica mora vzpostaviti evidenco vstopov in izstopov na varovanem območju.

16. člen

Obiskovalci se morajo obvezno javiti pri recepciji, se po potrebi predstaviti z osebnim dokumentom in povedati h komu so prišli in zakaj. Receptor obiskovalcu dovoli vstop praviloma v spremstvu uslužbenca.

V internih aktih posamezne družbe uporabnice je lahko določeno drugačno javljanje vstopa obiskovalcev, vendar mora biti zagotovljeni nadzor, opredeljen v tem členu.

17. člen

Receptor ali druga oseba, določena v internih aktih posamezne družbe uporabnice, mora voditi dnevnik obiskovalcev, v katerega se vpišejo ti podatki:

- ime in priimek,
- številka in vrsta osebnega dokumenta (po potrebi),
- čas prihoda,
- namen obiska (h komu),
- številka priponke »obiskovalec«, če je tako določeno v internem aktu posamezne družbe uporabnice,
- čas odhoda.

18. 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.

19. člen

Dostop uporabnikom na varovano območje je mogoč le v rednem delovnem času, zunaj tega časa pa samo na podlagi dovoljenja nadrejenega (pooblaščenega) zaposlenega.

Vsakršno odstopanje mora biti navedeno v internem aktu posamezne družbe uporabnice (npr. hišnem redu, načrtu varovanja).

Varovanje sredstev za dostop

20. člen

Vsak uporabnik 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.

21. člen

Morebitno krajo, izgubo ali založitev sredstva za dostop mora vsak uporabnik takoj prijaviti izdajatelju tega sredstva oziroma skrbniku za upravljanje teh sredstev v posamezni družbi uporabnici.

Varovanje opreme

Namestitev opreme

22. člen

Vsa oprema mora biti nameščena in zaščitena tako, da so nevarnosti iz okolja in priložnosti za nepooblaščeni dostop odpravljene v največji možni meri glede na dane okoliščine. Raven varovanja in zaščite mora biti določena glede na občutljivost podatkov in oceno tveganja izgube ali poškodovanja podatkov.

Protipožarno varovanje

23. člen

Protipožarno varovanje na varovanih območjih, na katerih je nameščena ključna in pomožna oprema, mora biti izvedeno v skladu s predpisi in navodili ustreznih pooblaščenih služb.

Zaščita ožičenja

24. 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 pri namestitvi opreme. Pri vsaki nadgradnji ali spremembi omrežja ali vanj vključenih naprav mora biti preverjena varnost ožičenja.

25. člen

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

26. 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.

27. člen

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

Okvare in poškodbe opreme

28. člen

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

2. Politika primerne rabe informacijskega sistema in zaščite občutljivih podatkov

Uporaba opreme informacijske tehnologije

29. člen

Informacijska in komunikacijska oprema JHL oziroma druge družbe uporabnice je namenjena opravljanju službenih obveznosti oziroma potrebam dela.

Uporaba v zasebne namene ni dovoljena, razen izjemoma za nujne zadeve in v manjšem obsegu, ki ne moti delovnega procesa, varnosti in razpoložljivosti IS.

30. člen

Uporabniki morajo z informacijsko opremo ravnati kot dober gospodar, po navodilih za uporabo od 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.

31. člen

Uporabniki ne smejo sami nameščati programske opreme razen z dovoljenjem odgovorne osebe. Nameščanje in vzdrževanje te opreme je v domeni skrbnikov IS.

Upravitelj IS mora poskrbeti, da so IS 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

32. člen

Namerno nameščanje ali uporaba zlonamerne programske opreme ali njeno širjenje je kršitev IVP JHL in hujša kršitev delovnih obveznosti. Namerno nameščanje, uporaba in širjenje take opreme se kaznuje v skladu z delovno pravnimi, odškodninskimi in kazenskimi predpisi.

Uporabniki:

- morajo, če sumijo, da na IS deluje zlonamerna programska oprema, takoj nehati delati z njim, obvestiti upravitelja IS in upoštevati njena navodila;
- morajo, če sumijo, da je na IS zlonamerna programska oprema, takoj obvestiti upravitelja IS in upoštevati njegova navodila;
- ne smejo zaganjati izvršljive programske opreme, ki ni del njihovega IS (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 IS, obvestiti upravitelja IS in upoštevati njegova navodila.

Informacijski sistem

33. člen

IS, ki obravnava občutljive podatke, nadzoruje upravitelj IS.

Nadzira se lahko tudi sistem, ki obravnava 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 poslovodje posamezne družbe uporabnice ali zahtevo pristojnega preiskovalnega organa v zvezi s sumom storitve kaznivega dejanja.

Podatki iz dnevnika se uporabljajo tudi za odkrivanje napak v IS ali za izboljšanje njegovega delovanja. V tem primeru zahteva za uporabo teh podatkov ni potrebna. V primeru, da dnevniki vsebujejo občutljive podatke, morajo biti zabeleženi vpogledi in ostali posegi na sistemu, skladno s predpisi.

34. člen

Uporaba zasebne opreme v IS ni dovoljena.

Upravljanje izmenljivih nosilcev podatkov

35. člen

Vsak uporabnik mora zagotoviti ustrezno varovanje in zaščito pri upravljanju izmenljivih nosilcev podatkov.

36. člen

Izgubo ali krajo izmenljivih nosilcev podatkov mora vsak uporabnik v čim krajšem času prijaviti nadrejenemu in skrbniku IS.

37. člen

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

38. člen

Uporabnik mora vse nosilce podatkov, ki jih ne potrebuje več oziroma so neuporabni, razdolžiti po postopku kot so opredeljeni v internih aktih.

Dostop do informacijskega sistema

39. člen

Za vsak IS mora biti vzpostavljen postopek dodelitve, sprememb in prenehanja dostopnih pravic.

40. člen

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

41. člen

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

42. člen

Dostop do IS 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.

43. člen

Sredstva za dostop do IS so neprenosljiva. Posojanje ni dovoljeno.

44. člen

Uporabnik mora skrbno varovati sredstva za dostop do IS, da se ne odtujijo ali zlorabijo.

Vsak sum zlorabe ali odtujitve je treba takoj prijaviti skrbniku IS.

45. člen

Dostop do storitev in upravljanja IS ter omrežja je mogoč po sistemu pravic. Te dodeljuje upravitelj IS ali omrežja ali pa v njegovem imenu izvajalec.

46. člen

Pravico dostopa do IS in vse spremembe teh pravic lahko pridobijo uporabniki ali administratorji na podlagi potreb iz delovnih obveznostih in odobritve nadrejenega. Če potreba po dostopu preneha, je treba to pravico odvzeti.

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

47. člen

Uporabniške in administratorske pravice dostopa do IS so ločene.

Zaposleni na svojih delovnih postajah ne smejo imeti administratorskih pravic.

Administratorske pravice imajo na delovnih postajah le pooblaščeni oziroma osebe, ki so odgovorne za delovanje IS.

48. člen

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

Načelo čiste mize

49. 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.

Načelo praznega zaslona

50. 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 aktom določeno drugače.

Oddaljeni dostop

51. člen

Oddaljeni dostop do IS je dovoljen le na podlagi odobrene metode z ustrezno ravnijo 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.

52. 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 družb uporabnic šifrira.

Dostop do svetovnega spleta in storitev v svetovnem spletu

53. člen

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

54. člen

Zaposleni morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami družb uporabnic oziroma posamezne družbe uporabnice. Vsi uporabniki IS se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom ene izmed družb uporabnic.

55. člen

Na podlagi ocene tveganja mora upravitelj IS poskrbeti za omejitve dostopa do vsebin zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev etičnih in moralnih norm.

56. člen

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

57. člen

V omrežju družb uporabnic 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 upravitelj IS posreduje le na obrazloženo zahtevo poslovodje posamezne družbe uporabnice, ki na podlagi zakonskih pooblastil obravnava domnevno nezakonita dejanja.

Drugačna obdelava podatkov iz prvega odstavka ni dovoljena. Rok hrambe teh sintetiziranih podatkov je tri mesece, nato se podatki uničijo ali anonimizirajo. Anonimizirani podatki se lahko uporabljajo za dvig kakovosti upravljanja IS.

58. člen

V omrežju družb uporabnic se na zahtevo poslovodje posamezne družbe uporabnice lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana.

Statistika se lahko uporablja za načrtovanje in varovanje IS.

Uporaba elektronske pošte

59. člen

Zaposleni 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.

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

60. 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 IS (zaupnost, celovitost in razpoložljivost).

61. 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. Seznam nedovoljenih priponk mora biti objavljen na običajen način v posamezni družbi uporabnici.

Pošiljanje obvestil o morebitnih novih virusih ni dovoljeno niti takrat, ko so prepričani, da ne gre za lažna obvestila. Obvestilo o sumljivi pošti se pošlje izključno upravitelju IS.

62. 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.

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 posamezne družbe uporabnice, razen če to ni povezano s potrebami delovnega mesta.

63. 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 upravitelja IS na naslov podpora@jhl.si ali po telefonu št. (01) 474 0444.

64. člen

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

65. 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

66. člen

Vse pravice na sistemu elektronske pošte in vseh elektronskih sporočilih, ki niso zasebna, pripadajo posamezni družbi uporabnici. Uporabniki se morajo zavedati, da se elektronska sporočila v sistemu elektronske pošte varnostno shranjujejo in bodo ostala shranjena tudi, če jih izbrišejo iz svojega elektronskega poštnega predala.

67. člen

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

68. 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 veljavnimi predpisi. Preusmeritev elektronske pošte v drug predal uporabnika ni dovoljena.

69. 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 poslovodje posamezne družbe uporabnice.

Pri tem se morajo upoštevati določila veljavnih standardov in predpisov ter internih aktov in vsa pravila, ki v takšnih primerih veljajo za ravnanje z gesli.

70. člen

Elektronska sporočila, ki prihajajo na enotne namenske elektronske poštne naslove (npr. glavna pisarna, projekt, sektor, podpora), odpirajo za to pooblaščene osebe.

Privzete nastavitve predala

71. člen

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

Velikost elektronskih sporočil

72. člen

Največja velikost sporočil pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena. Omejitev izhaja iz poslovnih potreb posamezne družbe uporabnice in priporočil upravitelja IS. Če je omejitev presežena, se sporočilo samodejno zavrne, pošiljatelj pa dobi obvestilo o zavrnitvi.

73. 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.

74. člen

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

75. 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.

76. člen

Pri ravnanju z občutljivimi podatki je treba dosledno upoštevati veljavne predpise, ki urejajo varstvo osebnih podatkov.

Šifriranje in podpisovanje elektronskih sporočil

77. člen

Šifriranje in podpisovanje elektronskih sporočil se lahko izvaja samo z uporabo odobrenih metod posamezne družbe uporabnice.

Brisanje elektronskih sporočil

78. člen

Vsak uporabnik mora vsa elektronska sporočila, ki jih ne potrebuje več, občasno brisati iz svojega predala oziroma mora to storiti na zahtevo upravitelja IS. 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.

79. člen

Nezaželeno pošto ima upravitelj IS pravico brisati.

Posebna pooblastila

80. člen

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

81. člen

Ob sumu storitve kaznivega dejanja z uporabo elektronskih sporočil, se opravijo postopki v skladu s predpisi po odredbi pristojnega državnega organa.

Pregledovanje elektronskih sporočil upravljavcev elektronske pošte iz radovednosti ali po nalogu nepooblaščenih posameznikov ni dovoljeno.

Dostop do podatkov

82. 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.

83. člen

Upravitelj IS ne sme imeti vpogleda v občutljive podatke, razen če ima za to ustrezna pooblastila.

84. člen

Vse zbirke občutljivih podatkov (elektronske in papirne) morajo imeti vzpostavljene ustrezne dnevnike vpogledov, v katerih je zabeleženo: kdo, kdaj in zakaj je opravil vpogled, skladno s predpisi, ki urejajo varstvo osebnih podatkov. Vodeni morajo biti tudi vsi servisni in vzdrževalni posegi na strežniku, bazi, aplikaciji ali storitvi.

85. 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).

86. člen

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

Podrobnejši postopek dodeljevanja dostopnih pravic za posamezni IS posamezne družbe uporabnice mora biti zapisan v internem aktu posamezne družbe uporabnice. Na centraliziranih informacijskih rešitvah morajo biti postopki dodeljevanja dostopnih pravic poenoteni.

87. člen

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

88. 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.

89. 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 s predpisi, ki urejajo varstvo osebnih podatkov in arhiviranje.

90. člen

Vsi uporabniki morajo varovati občutljive podatke, s katerimi so se seznanili med trajanjem delovnega oziroma pogodbenega razmerja. Varovati jih morajo tudi po prenehanju tega razmerja.

3. Politika nabave opreme in storitev pri zunanjih izvajalcih

Priprava javnega naročila

91. člen

Pri pripravi specifikacij javnega naročila za nabavo gradnikov ali vzdrževanje IS je treba predvideti in opredeliti varnostne elemente, ki bodo izpolnjevali zahteve IVP JHL in veljavne predpise in standarde.

92. člen

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

93. člen

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

94. člen

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

Varnostni elementi v pogodbi

95. 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 IVP JHL 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 IVP JHL in sprejemanju te politike.

Za veljavne pogodbe, sklenjene pred uveljavitvijo IVP JHL, je treba z izvajalci skleniti ustrezne dodatke k pogodbam in podpisati izjave, kjer je to smiselno in izvedljivo.

96. člen

V pogodbi ali drugem aktu morata biti, če je to potrebno, določena način fizičnega dostopa do informacijskega premoženja družbe uporabnice oziroma posamezne družbe uporabnice in način prijave v IS.

Podeljene pravice dostopa do informacijskega premoženja 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 IS morajo biti beleženi.

97. 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.

98. člen

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

99. člen

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

100. člen

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

Izvajanje pogodbe

101. 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

102. člen

Naročnik in izvajalec določita skrbnike pogodb, ki skupaj z upraviteljem IS sproti preverjajo ustreznost v pogodbi opredeljene storitve.

Zunanji izvajalec mora skrbniku pogodbe redno dostavljati poročila o njenem izvajanju.

103. člen

Zunanji izvajalec rešitve, ki jih je namensko razvil za posamezno družbo uporabnico in bi uporaba zunaj družbe lahko ogrozila varnost IS, ne sme dati naročnikom zunaj družbe.

4. Politika razvoja in vzdrževanja informacijskega sistema in obvladovanja sprememb

Načrtovanje

104. člen

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

105. člen

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

106. člen

Novi IS oziroma njegov del mora biti skladen z varnostnim standardom v IS družb uporabnic.

107. člen

Kakršne koli spremembe IS smejo biti izvedene le na podlagi naročila lastnika sistema.

Postopek upravljanja sprememb in same spremembe morajo biti dokumentirane.

Razvojno okolje

108. 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.

109. člen

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

110. 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.

111. člen

Uporaba produkcijskih podatkov v razvojnem okolju ni dovoljena.

Testno okolje

112. člen

Testno okolje mora biti v upravljanju in pod nadzorom upravitelja IS.

113. člen

Nameščanje in spreminjanje strojne opreme, aplikacij in zbirk podatkov mora naročati, odobriti in nadzirati od upravitelja IS imenovan skrbnik.

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.

114. člen

Naročnik mora preveriti in potrditi funkcionalnost, varnost in zmogljivost same aplikacije ali strojne opreme, aplikacije ali strojne opreme v povezavi z IS in vpliv na IS.

115. 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, razen za testne namene.

Izobraževalno okolje

116. 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.

Produkcija

117. člen

O pogojih za izvedbo sprememb v produkcijskem okolju se dogovorita naročnik in skrbnik IS.

Spremembe, ki zahtevajo prekinitev v delovanju IS, morajo biti načrtovane in vnaprej napovedane.

Vsako izvedeno spremembo je treba evidentirati.

118. člen

Vzpostavljen in dokumentiran mora biti postopek prenosa programske in/ali strojne opreme v produkcijsko okolje za vsak del IS. Postopek mora vključevati uporabniške in zmogljivostne teste z dokazili o izpolnjevanju naročnikovih zahtev.

Priloženo mora biti potrdilo, da spremembe ne vplivajo na delovanje drugih delov IS in da so v IS vgrajeni vsi zahtevani varnostni elementi.

Postopek prenosa mora biti pod nadzorom.

119. 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.

120. člen

Za poslovno kritične informacijske rešitve mora biti praviloma vzpostavljen postopek preverjanja programske kode zaradi preprečitve znanih varnostnih pomanjkljivosti v programski kodi.

121. člen

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

Pravice dostopa

122. člen

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

123. člen

Dostop do produkcijskih podatkov v IS je zunanjim izvajalcem prepovedan. Izjemoma jim je lahko dovoljen pod nadzorom naročnika oziroma upravitelja IS in na podlagi njegove zahteve, ki velja le za posamezen primer in v omejenem obsegu.

124. člen

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

125. člen

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

126. člen

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

5. Politika upravljanja informacijskega sistema

Upravljanje produkcijskega okolja

127. člen

Produkcijska okolja IS morajo biti pod nadzorom in v upravljanju upravitelja IS.

Storitve upravljanja produkcijskega okolja lahko izvajajo zunanji izvajalci, ki imajo sklenjene pogodbe o dobavi storitev.

128. člen

Naloga upravitelja IS je, da poskrbi za njegovo delovanje z zagotavljanjem varnosti (zanesljivost, celovitost in razpoložljivost).

129. člen

Za informacijsko omrežje in njegovo varnost je zadolžen skrbnik omrežja, ki ga imenuje upravitelj IS. Skrbnik omrežja 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.

Dokumentirani delovni postopki

130. člen

Postopki, ki so povezani z delovanjem IS, morajo biti dokumentirani. Za to mora poskrbeti upravitelj IS.

Ob spremembah postopkov je treba posodobiti tudi dokumentacijo. Ta mora biti pregledana vsaj enkrat na leto in biti na voljo na kraju uporabe.

Upravljanje sprememb v produkcijskem okolju in omrežju

131. člen

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

132. člen

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

Ločevanje nalog

133. člen

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

Zaščita pred zlonamerno in prenosno kodo

134. člen

Informacijsko omrežje družb uporabnic mora imeti vgrajene mehanizme, ki omogočajo zaznavanje in preprečevanje zlonamerne programske opreme že na mrežni ravni, če to ni urejeno s priklopom v prostrano omrežje družb uporabnic.

Mehanizme za zaznavanje in preprečevanje zlonamerne programske opreme morajo imeti tudi zasebna omrežja, ki se priklapljajo v prostrano omrežje družb uporabnic.

Časovna uskladitev

135. člen

Za sinhronizacijo dnevniških zapisov v IS je obvezno treba uporabljati sistem enotnega izvora časa.

Nadzor dostopa do omrežja

136. člen

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

Ločevanje v omrežjih

137. 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 veljavnih predpisov in standardov ter varnostnih zahtev v vseh omrežjih.

Upravljanje omrežnega usmerjanja

138. člen

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

Upravljanje incidentov pri varovanju informacij

139. člen

Upravitelj IS mora zagotoviti, da se dejavnosti in dogodki v IS beležijo.

Na podlagi ugotovljenih dogodkov mora izvajati ustrezne ukrepe.

140. člen

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

141. člen

Voditi je treba zapise o incidentih.

Dnevniški zapisi

142. člen

Redno se izdelujejo dnevniški zapisi o spremembah in posegih v IS. Obseg podatkov v dnevniških zapisih in rok hrambe morata biti sorazmerna z namenom beleženja in morata upoštevati določbe veljavnih predpisov.

Redno se izločajo stari dnevniški zapisi.

143. člen

Zagotovljeni morata biti celovitost in nespremenljivost dnevniških zapisov, ki jih pregleduje upravitelj IS za potrebe upravljanja IS ali omrežja.

Dostop do dnevniških zapisov imajo za to pooblaščene osebe upravitelja IS in druge osebe ob upoštevanju omejitev, ki jih določajo predpisi s področja varstva osebnih podatkov in interni akti.

Postopki in ukrepi morajo onemogočati možnost spreminjanja ali nepooblaščenega izklopa revizijskih sledi (podatkov v dnevnikih).

Obdelava podatkov v dnevniških zapisih

144. člen

Dnevniški zapisi, ki vsebujejo občutljive podatke, se hranijo, obdelujejo in pošiljajo skladno z veljavnimi predpisi, 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.

Ravnanje na podlagi ugotovitev iz dnevniških zapisov

145. člen

Na podlagi sporočil posameznega dela IS ali posameznih mrežnih naprav se izločajo dnevniški zapisi, ki nakazujejo napako na napravi ali nedovoljeno dejavnost. Upravitelj IS 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 IS.

146. člen

Neodobrene mrežne opreme ni dovoljeno priklapljati v omrežje. Skrbnik lokalnega omrežja mora zagotoviti mehanizme za odkrivanje nedovoljenih mrežnih naprav.

Kriptografske rešitve

147. člen

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

148. člen

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

149. 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 upravitelj IS glede na skladnost z varnostnimi elementi, ki zagotavljajo varnostno ustreznost.

Raba virov

150. člen

Raba vseh virov, ki so vključeni v delovanje produkcijskega okolja, mora biti spremljana in upravljana tako, da omogoča zahtevano kakovost storitve. Poslovodje družb uporabnic morajo zagotoviti ustrezne vire za nemoteno delovanje skladno z načrtom neprekinjenega poslovanja oziroma skladno z ukrepi, ki izhajajo iz ocene tveganj.

Oskrba z električno energijo

151. člen

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

Klimatski pogoji

152. člen

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

Varnostne kopije

153. člen

Varnostne kopije podatkov v IS morajo biti izdelane, hranjene in preverjane skladno z oceno tveganja in zahtevami upravitelja IS. Zahteve vsebujejo informacijo o podatkih, ki jih mora vsebovati 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.

154. člen

Varnostne kopije morajo biti varno hranjene tudi na oddaljeni lokaciji. Pri njihovem prenosu morajo biti izpolnjeni zahtevani varnostni pogoji.

155. člen

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

Upravljanje neprekinjenega poslovanja

156. člen

Poslovni procesi v družbi, ki so podprti z IS, morajo imeti dokumentiran postopek – načrt neprekinjenega poslovanja, ki opredeljuje:

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

157. člen

Skrbniki načrtov neprekinjenega poslovanja so lastniki procesov.

158. 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 IS, morajo skupaj z upraviteljem IS 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 poslovodje družb uporabnic.

159. člen

Prednostne naloge pri reševanju IS ob morebitni večji katastrofi se določijo na podlagi ocene tveganj.

160. člen

IS, katerih nedelovanje ima velike posledice za družbe uporabnice oziroma posamezno družbo uporabnico, morajo imeti podvojeno infrastrukturo na oddaljeni lokaciji. Ta mora zagotavljati izvajanje procesov z enako stopnjo varnosti (rezervna lokacija).

161. člen

Skrbniki IS morajo redno vzdrževati produkcijsko okolje in omogočati njegovo neprekinjeno delovanje. Poslovodje družb uporabnic v sodelovanju z upraviteljem IS morajo skupaj načrtovati razvoj infrastrukture in zagotavljati vire za njeno nemoteno delovanje.

162. člen

Informacijsko omrežje družb uporabnic mora biti grajeno tako, da se ob izpadu glavne povezave vzpostavi nadomestna povezava.

Vzdrževanje opreme

163. 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.

164. člen

Za vsak kos opreme, ki zapusti družbo uporabnico zaradi vzdrževanja, je treba imeti prevzemni dokument.

Vzdrževalna dela

165. člen

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

Prehodne in končne določbe

166. člen

IVP JHL začne veljati 10.12.2013.

Interne akte oziroma dokumente je potrebno uskladiti z določbami IVP JHL v roku enega leta od uveljavitve te IVP JHL.

Izvedbeni akti oziroma dokumenti iz te IVP JHL morajo biti pripravljeni v roku enega leta od uveljavitve te IVP JHL.

IVP JHL se objavi na intranetni strani oziroma na običajen način.

Številka: 1249-P/2013
Ljubljana, dne 29.11.2013

Direktorica
Zdenka Grozde, univ. dipl. prav.

Javni holding Ljubljana
JAVNI HOLDING Ljubljana, d.o.o.
Verovškova ulica 70, 1000 Ljubljana