

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, 38/10, 101/10 in 81/13), Priporočil informacijske varnostne politike javne uprave (št. 386-2/2008/23 z dne 28. 10. 2010), 51. in 89. člena Statuta Mestne občine Ljubljana (Uradni list RS, št. 24/16 – uradno prečiščeno besedilo) in 4. člena Odredbe o varnostni politiki št. 386-1/2010-19 z dne 24. 4. 2018 izdaja župan Mestne občine Ljubljana

PRAVILNIK O VAROVANJU INFORMACIJSKEGA SISTEMA

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se v Mestni občini Ljubljana (v nadaljnjem besedilu: MOL) določa:

- način upravljanja uporabniških računov, s katerimi se dostopa do informacijsko komunikacijske tehnologije v lasti, upravljanju ali uporabi MOL (v nadaljnjem besedilu: sredstva MOL);
- način uporabe informacijskega sistema MOL;
- način dostopa do podatkov MOL, upravljanje z incidenti, ter oddaljen dostop.

2. člen

Cilji tega pravilnika so:

- izboljšati varovanje vseh informacij v MOL;
- dodeliti vloge in odgovornosti zaposlenim in študentom na posameznih področjih v MOL, da skrbijo za varovanje informacij;
- dodeliti vloge in odgovornosti zunanjim izvajalcem, da skrbijo za varovanje informacij;
- povečati informacijsko-varnostno osveščenost vseh zaposlenih, študentov ter drugih zunanjih izvajalcev in tako zmanjšati vpliv varnostnih groženj.

3. člen

K ravnanju skladno s tem pravilnikom se skladno s 5. členom Odredbe o varnostni politiki s pogodbo oziroma izjavo zaveže tudi zunanje izvajalce, ki uporabljajo sredstva MOL (v nadaljnjem besedilu: zunanji izvajalec). Obiskovalce se k ravnanju skladno s tem pravilnikom na ustrezen način seznani.

4. člen

Pojem »organ mestne uprave« se smiselno uporablja tudi za Službo za notranjo revizijo.

5. člen

Vprašanja o pravilnem ravnanju s sredstvi MOL se naslavljajo na Center za informatiko (v nadaljnjem besedilu: CI).

II. UPORABNIŠKI RAČUNI

6. člen

Za uporabo in upravljanje informacijskih sistemov se v MOL uporabljata dve vrsti računov: skrbnik in uporabnik. Kategoriji definirata splošne odgovornosti z ozirom na informacijsko varnost. Skrbniki za vzdrževanje sistemov uporabljajo dodaten skrbniški račun.

7. člen

Uporabniki delovnih postaj in prenosnih računalnikov nimajo skrbniških pravic in ne nameščajo programske opreme. Izjeme so uporabniki, ki, glede na naravo dela, potrebujejo na delovni postaji ali prenosnem računalniku skrbniške pravice. Seznam izjem se vodi v CI.

Uporabniki sredstev MOL so dolžni redno odstranjevati nepotrebno elektronsko gradivo.

Uporaba sredstev MOL 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 vodja organa mestne uprave ali poslovodni organ druge osebe javnega prava, ki uporablja sredstva MOL na podlagi akta iz drugega odstavka 17. člena trga pravilnika.

Shranjevanje privatnih datotek (slikovno gradivo, multimedijske vsebine, ...) na sredstvih MOL ni dovoljeno, oziroma so lahko izjemoma privatne datoteke shranjene le v mapi na lokalnem disku osebnega računalnika, katerega uporablja uporabnik in le v obsegu, da velikost te mape ne zmanjšuje uporabnost osebnega računalnika. Takšno mapo je potrebno jasno označiti (npr. mapa „Zasebno“), sicer se bo štela kot poslovna mapa in je lahko predmet dostopa delodajalca. Prav tako delodajalec ne prevzema nikakršne odgovornosti pred izgubo privatnih datotek.

8. člen

Skrbnik ima pravice nameščanja programske opreme. Loči se več nivojev skrbnikov: skrbnik delovnih postaj in prenosnih računalnikov ter skrbnik sistemov.

Skrbnik je zavezan k odgovornosti do varovanja podatkov in upoštevanju splošnih moralnih vodil. Skrbnik v ta namen podpiše izjavo. Seznam skrbnikov vodi CI.

9. člen

Odsek za upravljanje s kadri skrbnikom, ki upravljajo z uporabniškimi računi in pravicami dostopa, posreduje podatke o vseh kadrovskih spremembah, ki vplivajo na proces prijave ali odjave ter vpis novega uporabnika informacijskega sistema. Na podlagi prejetih podatkov skrbnik spremeni, blokira oziroma pripravi nov račun ter posreduje podatke zaposlenemu, študentu oziroma drugemu zunanjemu izvajalcu.

Za vsak informacijski sistem oziroma storitev, ki dostop ureja s sistemom uporabniških in skrbniških računov, mora biti s strani skrbnika opredeljen postopek upravljanja z računi. Skrbnik mora aktivnosti izvajati v skladu z opredeljenim postopkom.

10. člen

Skrbnik pogodbe na strani MOL je odgovoren za izvajanje nadzora nad ustreznostjo pravic dostopa zunanjega izvajalca v informacijskih sistemih.

Pravice dostopa zunanjega izvajalca preverja vodja organa mestne uprave, kot je to določeno v drugem odstavku 6. člena Pravilnika o upravljanju uporabniških računov.

Nadzor nad uporabniškimi računi študentov izvaja vodja organizacijske enote, v kateri študent dela (v nadaljnjem besedilu: odgovorna oseba). Odgovorna oseba pripravi predlog spremembe dostopnih pravic na podlagi obrazca o dodelitvi sredstev MOL in pravic dostopa ter ga posreduje vodji organa mestne uprave v odobritev. Odgovorna oseba po potrditvi predloga obrazec s podatki posreduje v Odsek za upravljanje s kadri ter CI. CI izvede zahtevo.

Odgovorna oseba za delo študenta je odgovorna za natančno vodenje evidence vseh sprememb pravic dostopa študenta.

11. člen

Pripravo skrbniškega računa odobri vodja CI.

12. člen

Dodelitev pravic dostopa zaposlenim in študentom se izvede, kot je to določeno v drugem odstavku 5. člena Pravilnika o upravljanju uporabniških računov.

Dodelitev pravic dostopa zunanjim izvajalcem se izvede, kot je to določeno 6. členu Pravilnika o upravljanju uporabniških računov.

Vsi zaposleni, študentje in drugi zunanji izvajalci v MOL uporabljajo za prijavo v sistem identifikacijo. Uporabniško ime je sestavljeno v skladu s pravili. Glede na dodeljene pravice zaposleni, študent ali drug zunanji izvajalec dostopa do podatkov, ki jih potrebuje za opravljanje svojega dela.

13. člen

Med prijavo je mogoča večkratna napačna prijava. Vsak uporabnik sistemov, s katerimi upravlja MOL, je osebno odgovoren za uporabo svojega računa. Odgovoren je za vsa dejanja, ki so izvedena z njegovim računom. V primeru suma, da je prišlo do razkritja gesla, ga je potrebno nemudoma spremeniti.

14. člen

Identifikacija zagotavlja, da je vsakršna aktivnost povezana s točno določenim posameznikom. CI vodi seznam uporabnikov.

15. člen

Dostop do uporabniškega računa je nadzorovan. Vsi dostopi se zapisujejo v dnevniku dostopov. Kontrole dostopa do podatkov in drugih informacijskih virov (dnevnik dela računalnika) omogočajo naknadno ugotavljanje dostopov. Dnevnike nadzira skrbnik, ki določa tudi vsebino zapisa v dnevniku. Na zahtevo vodje organa mestne uprave izpiše podatke iz dnevnika.

16. člen

Vsa gesla in postopki, ki se uporabljajo za vzdrževanje sistemov, se hranijo v CI. Način hranjenja določi vodja CI. Gesla se uporabijo samo v izrednih okoliščinah oziroma ob nujnih primerih. Po vsaki uporabi se geslo zamenja.

III. INFORMACIJSKI SISTEM

17. člen

Sredstva MOL se uporabljajo le v službene namene MOL, kolikor ni s tem ali drugim aktom drugače določeno.

Sredstva MOL druge osebe javnega prava uporabljajo pod pogoji, ki jih opredeljuje ustanovitveni ali drug akt v skladu z veljavnimi predpisi. Pri tem morajo v celoti privzeti določila informacijske varnostne politike MOL in upoštevati s strani CI opredeljene Splošne pogoje za uporabo storitev podatkovnega centra MOL ter posebna določila in omejitve, ki za te primere veljajo za konkretne storitve.

18. člen

Dejanja, ki motijo normalne in dovoljene operacije na sistemih, škodijo ugledu MOL in žalijo druge, so strogo prepovedana in predstavljajo kršitve delovnih obveznosti. Neprimerna dejanja vodijo do disciplinskih ukrepov.

19. člen

Informacijski sistemi in aplikacije se preverjajo. Za uporabo so dovoljene le tiste aplikacije, ki so opredeljene v katalogu informacijskih storitev in prevzete v upravljanje s strani CI.

Pravila nadzora sistema in vključevanje naprav ter informacijskih storitev v omrežje MOL izvaja CI.

20. člen

Delovne postaje, prenosni računalniki in strežniki, ki so priključeni na mrežo, so identificirani. Vsako sredstvo MOL ima svojo identifikacijsko številko.

21. člen

V MOL je določen standardni seznam dovoljenih paketov programske opreme, ki jo zaposleni, študentje in drugi zunanji izvajalci lahko uporabljajo. Programske opreme, ki ni na seznamu, ni dovoljeno nameščati. Programsko opremo lahko namešča le skrbnik.

22. člen

Na sredstvih MOL je prepovedano spreminjanje sistemskih nastavitev, nadgrajevanje obstoječih operacijskih sistemov ali nameščanje novih operacijskih sistemov. Omenjene aktivnosti izvajajo lahko le izvajalci, pooblaščen s strani CI.

23. člen

Programska oprema, ki se namešča v omrežje MOL, se mora pridobiti od zaupanja vrednih dobaviteljev ter predhodno testirati s strani proizvajalca ali dobavitelja ter prevzemno testirati s strani CI.

24. člen

Dostop do testnih in sistemskih podatkov imajo samo skrbniki v CI.

25. člen

Nadgradnje se izvajajo zaradi potreb po novi funkcionalnosti ter nameščanja popravkov. Programski paketi se nadgrajujejo, ko za slednje obstajajo potrebe. Kjer je to mogoče, nadgradnje potekajo avtomatsko. Takšen primer so delovne postaje ter prenosni računalniki. Drugje, kot so strežniški sistemi, se nadgradnje izvajajo ročno, ko obstaja potreba po tem. Nameščanje popravkov se evidentira in spremlja. Skrbniki spremljajo, kateri so kritični popravki. Nameščanje popravkov se spremlja in vodi po postopku vpeljave sprememb. Ob spremembah na operacijskih sistemih se ta testira v testnem okolju, kolikor je to mogoče. Po uspešno opravljenem testiranju se nadgradnja namesti v produkcijsko okolje.

26. člen

Spremembe na sistemih, za katere skrbi zunanji izvajalec, se izvajajo skladno s pogodbenimi zahtevami.

27. člen

Spremembe na programski ali strojni opremi se beležijo v CI. Večjo spremembo na sistemu odobri vodja CI. Zahteve po spremembah na delovni postaji ali prenosnem računalniku v CI posreduje zaposleni po predhodni odobritvi vodje organa mestne uprave.

28. člen

Uvajanje novih sistemov se izvaja na podlagi projektne metodologije, ki jo opredeli CI.

29. člen

CI stalno nadzira omrežja, s katerimi upravlja MOL, in omrežni promet s pomočjo nadzornih orodij in drugih dobrih praks. Posamezni dogodki na omrežjih CI se evidentira v dnevnikih naprav ali nadzornega sistema. V primeru ugotovljenih neskladnosti nadzorni sistemi avtomatsko obvestijo skrbnika sistema.

30. člen

MOL ima s ponudniki omrežnih storitev podpisano pogodbo o zagotavljanju storitev. Pogodba vključuje nivoje storitev, zahteve glede upravljanja storitev ter ustrezne varnostne kontrole. CI redno nadzira, ali ponudnik omrežnih storitev dogovorjene storitve upravlja na varen način.

31. člen

Vsa programska oprema se pred namestitvijo in uporabo arhivira. Arhivske kopije in dokumentacija o licencah programske opreme se hranijo v CI. Dokumentacija o licencah za programsko opremo se hrani z namenom izvajanja tehnične podpore, nadgradnje opreme ter dokazovanja veljavnosti licenc.

32. člen

Nepooblaščenno kopiranje licenčne in avtorsko zaščitene programske opreme je prepovedano. Reprodukcijska avtorsko zaščitena materiala je dovoljena le v primeru, da je uradno sprejemljiva ali z dovoljenjem avtorja.

33. člen

Za vse občutljive, dragocene ali kritične informacije v papirni in elektronski je zagotovljeno varnostno kopiranje. Za opredelitev operativnih postopkov je odgovoren skrbnik storitve.

34. člen

Sistemska dokumentacija v elektronski ali papirni obliki hrani in varuje pred nepooblaščenim dostopom CI.

IV. DOSTOP DO PODATKOV

35. člen

Vsi sistemi v MOL imajo nameščene mehanizme za kontrolo dostopa, kot je to določeno v 4. členu Pravilnika o upravljanju uporabniških računov.

36. člen

Posebnosti dostopov so opredeljene v navodilih posameznega sistema.

37. člen

Uporabnikove pravice dostopa se redno in v določenih intervalih preverjajo s strani skrbnika. Pregledi se opravljajo najmanj enkrat letno. Izredno zahtevo za pregled dostopnih pravic lahko zahteva vodja organa mestne uprave.

V. UPRAVLJANJE Z INCIDENTI

38. člen

O vsakem sumu zlorabe tega in drugih pravilnikov se ukrepa skladno z 8. členom Odredbe o varnostni politiki.

Okvare programske opreme se prijavijo na Enotno vstopno točko (v nadaljnjem besedilu: EVT).

V primeru suma, da je okvara nastala zaradi zlonamerne programske opreme ali nedovoljenih uporabniških aktivnosti, skrbnik dogodek podrobno razišče in o ugotovitvah poroča vodji CI.

39. člen

Zaposleni, študentje in drugi zunanji izvajalci ne testirajo ali poskušajo kompromitirati varnostnih zapor v računalniški ali komunikacijski sistem. Med takšne incidente se šteje tudi nedovoljeno vdiranje v sistem, ugibanje gesel, dešifriranje datotek, kopiranje programske opreme in podobni nedovoljeni poskusi vdora.

40. člen

EVT vodi evidenco incidentov ter posledic incidentov. Pri večjih incidentih in okvarah se pripravi poročilo in seznam korektivnih ukrepov.

41. člen

Pri vsakem incidentu se zbira dokaze, da se lahko v primeru, ko je to potrebno, z njimi podpre proces proti storilcu. Zbirajo se le oprijemljivi dokazi. V primeru da je to potrebno se za zbiranje dokazov vključi tudi zunanja inštitucija.

VI. ODDALJEN DOSTOP

42. člen

Oddaljen dostop je mogoč samo na podlagi odobrenega zahtevka. Oddaljen dostop odobri vodja CI. Evidenca dostopov se vodi v CI.

Možnosti za oddaljen dostop imajo lahko tudi zunanji izvajalci. Dostop se odobri na podlagi narave dela. Predlaga ga kontaktna oseba izvajalca na strani MOL, pripravi se v CI.

VII. KONČNA DOLOČBA

43. člen

Ta pravilnik začne veljati naslednji dan po objavi na intranetni strani MOL.

Številka: 386-1/2010-21

Datum: 24-04-2018

Župan
Mestne občine Ljubljana
Zoran Janković



12