

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), 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 UPORABI RAČUNALNIŠKE IN KOMUNIKACIJSKE OPREME TER MOBILNIH NAPRAV PRI ODDALJENEM DOSTOPU

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določijo postopki za dodelitev računalniške in komunikacijske opreme ter mobilnih naprav (mobilni telefoni, dlančniki in tablični računalniki z dostopom do podatkov prek mobilnega ali brezžičnega omrežja) za podporo oddaljenega dostopa in dostopom do internih podatkov zaposlenih v Mestni upravi Mestne občine Ljubljane (v nadaljnjem besedilu: mestna uprava) in zunanjih izvajalcev, ki uporabljajo predpisana sredstva Mestne občine Ljubljana, (v nadaljnjem besedilu: zunanji izvajalci).

Pojem »oddaljen dostop« se uporablja za vse primere, ko uporabnik iz prejšnjega odstavka (v nadaljnjem besedilu: uporabnik) uporablja komunikacijsko, računalniško opremo ali mobilno napravo Mestne občine Ljubljane (v nadaljnjem besedilu: MOL), ki ni povezana v lokalno računalniško omrežje MOL.

Pojem »dostop do internih podatkov« se uporablja za šifriran in z uporabniškim imenom in geslom zavarovan dostop do naslednjih internih podatkov: službene elektronske pošte in vsebine na intranetnih straneh MOL.

Pojem »varovani podatki« se uporablja za podatke, za katere zakonodaja predpisuje organizacijske in tehnične postopke za preprečevanje razkritja nepooblaščenim osebam (kot npr. osebne podatke, tajne podatke, poslovne skrivnosti in morebitne druge varovane podatke).

2. člen

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

II. DODELITEV OPREME

3. člen

Dodelitev opreme je le možnost in ne splošna ugodnost uporabnikov. Če vodja organa mestne uprave meni, da bo delo učinkovito izvedeno izven uradnih prostorov MOL ter da ima uporabnik delovne navade, primerne za oddaljen dostop, pošlje direktorju mestne uprave zahtevek za dodelitev pravic za oddaljen dostop, ki opredeljuje ustrezno računalniško in komunikacijsko opremo oziroma mobilno napravo ter pravice oddaljenega dostopa za delo določenemu uporabniku. Če direktor mestne uprave zahtevku ugodi, Center za informatiko (v nadaljnjem besedilu: CI) preda ustrezno opremo in zagotovi ustrezne pravice.

V Obrazcu o dodelitvi sredstev in pravic iz zadnjega odstavka 5. člena Odredbe o varnostni politiki se opredeli delo, ki ga bo opravljal uporabnik prek oddaljenega dostopa, oprema, ki jo prejme uporabnik, čas uporabe opreme ter pravice glede na vrsto uporabniškega računa.

4. člen

MOL ima, ob predhodnem opozorilu uporabnika, pravico do izvajanja oddaljenega nadzora delovne postaje ali prenosnega računalnika oziroma mobilne naprave uporabnika, ki opravlja delo prek

oddaljenega dostopa. MOL ima tudi pravico, da ob navzočnosti uporabnika pregleda vsebine katerega koli računalnika oziroma mobilne naprave v lasti MOL, ki vsebuje ali naj bi vseboval interne podatke MOL.

5. člen

Podatki MOL se ves čas varujejo, sorazmerno z njihovo klasifikacijo. Varnostni ukrepi se upoštevajo ne glede na medij, na katerem so podatki zapisani, lokacijo, kjer je informacija shranjena, sistem, s katerim se informacija obdeluje, uporabnike, ki imajo dostop do informacije, ali postopke, s katerimi se informacija obravnava. To pomeni, da morajo uporabniki varovati podatke in naprave na enak način, ne glede na to, ali se nahajajo v uradnih prostorih MOL ali na drugi lokaciji

6. člen

Uporabniki, ki uporabljajo oddaljen dostop, morajo svojega nadrejenega in CI nemudoma obvestiti o nastanku škode na računalniški ali komunikacijski opremi ali mobilni napravi o izgubi opreme, programov ali podatkov MOL, ki so bili zaupani v njihovo oskrbo.

7. člen

CI, v skladu s tehničnimi možnostmi in s priporočilom Informacijske pooblaščenke RS, lahko zagotovi varno upravljanje mobilnih naprav na daljavo s sistemom za upravljanje mobilnih naprav.

III. KONTROLA DOSTOPA

8. člen

Računalniki MOL, ki se uporabljajo pri oddaljenem dostopu in vsebujejo varovane podatke, morajo imeti nameščeno možnost šifriranja na trdem disku za vse podatkovne datoteke in zaščito z geslom.

9. člen

Računalnike in mobilne naprave MOL lahko uporabljajo zgolj uporabniki. Družinski člani in tretje osebe ne smejo uporabljati teh naprav.

IV. ARHIVIRANJE IN HRANJENJE MEDIJEV

10. člen

Naloga uporabnikov, ki uporabljajo oddaljen dostop, je tudi arhiviranje podatkov, ki se pridobijo izven uradnih prostorov MOL. Uporabnik, ki uporablja računalnik oziroma mobilno napravo v lasti MOL izven uradnih prostorov MOL, mora vse pomembne podatke ob prihodu na delovno mesto varno shraniti.

11. člen

Ko uporabnik pri oddaljenem dostopu zapiše podatek na disketo, magnetni trak, CD/DVD ROM, USB ključ ali drug pomnilni medij, ga mora označiti s stopnjo zaupnosti glede na najvišje klasificiran podatek, vsebovan na istem mediju. Ta medij uporabnik dostavi v MOL in shrani ustrezno s stopnjo zaupnosti.

V. KOMUNIKACIJSKE POVEZAVE

12. člen

Uporabniku se pri oddaljenem dostopu po potrebi zagotovi oskrba z ustrezno komunikacijsko opremo, vključno z varovanjem oddaljenega dostopa. Uporabnik je povezan z omrežjem preko šifrirane povezave. Za vzpostavitev te povezave se uporabnik identificira z uporabniškim certifikatom ali uporabniškim računom.

Uporabniki ne smejo puščati nenadzorovanih računalnikov z vključeno povezavo in komunikacijsko programsko opremo.

13. člen

Klicno ali internetno povezavo za dostop do interneta in elektronske pošte lahko uporabnik, ki uporablja oddaljen dostop, vzpostavi le, če ima za to dodeljene pravice. Računalnik mora imeti nameščen protivirusni program s požarnim zidom.

14. člen

Uporabniki se morajo izven uradnih prostorov MOL izogibati telefonskim pogovorom o varovanih podatkih. Če je takšen pogovor nujen, morajo uporabniki paziti, da po nepotrebem ne omenjajo zaupnih podrobnosti.

VI. UPRAVLJANJE SISTEMA

15. člen

Uporabniki ne smejo prinašati v prostore MOL lastnih računalnikov z namenom, da bi upravljali ali drugače ravnali z informacijami MOL.

16. člen

Uporabniki dostopajo do strežnikov v MOL preko šifrirane povezave.

17. člen

Računalniki se fizično zaščitijo pred dostopom. Na vsakem računalniku se lokalno namesti protivirusna programska oprema.

Računalnik mora imeti vključen lokalni požarni zid. Protivirusno programsko opremo je treba redno posodablјati. Opravljati je treba stalni nadzor nad funkcijami, ki jih opravlja računalnik, preden se priključi v omrežje, pa je treba preveriti lastnosti omrežja.

Po tem, ko uporabnik zaključi delo, se odjavi in prekine povezavo.

18. člen

Pri mobilnih napravah je potrebno poskrbeti za to:

- da so le-te nenehno pri uporabniku;
- da imajo nastavljeno zaščitno geslo za vklop in časovno nadzorovan izklop;
- da je omogočeno šifriranje podatkov, kjer je to mogoče;
- da konfiguracija dostopa do elektronske pošte mora omogočati ukinitve oddaljenega dostopa;
- da v primeru odtujitve naprave CI v skladu s tehničnimi možnostmi zagotovi brisanje poslovnih informacij in zaklepanje mobilne naprave na daljavo.

19. člen

Za vse spremembe na programski opremi skrbi CI. Pri tem prepozna vsa področja, na katera vpliva sprememba in obvesti uporabnike, na katere bo sprememba verjetno vplivala.

Uporabnik lahko naredi spremembo na programski opremi le v izjemnih primerih in to z dovoljenjem CI.

VII. UNIČENJE VAROVANIH PODATKOV

20. člen

Uporabnik ne sme odstraniti varovanih podatkov, shranjenih na pomnilnikih računalnikov, disketah, CD/DVD-ROM-ih, USB ključih ter drugih pomnilniških medijih in papirnih zapisih, brez vnaprejšnje privolitve vodje organa mestne uprave.

VIII. FIZIČNA VARNOST

21. člen

Uporabniki morajo na lokacijah izven uradnih prostorov MOL izvajati potrebne ukrepe za zaščito računalniške in komunikacijske opreme ter mobilnih naprav, programske opreme ter podatkov v lasti MOL pred krajo, poškodbami in zlorabo.

22. člen

Uporabniki, ki zaradi svojega dela občasno hranijo varovane podatke MOL na svojem domu, jih morajo hraniti varno.

23. člen

Uporabniki, ki uporabljajo oddaljen dostop na službeni poti ne smejo metati varovanih podatkov v hotelske koše za smeti ali druge javno dostopne smetnjake. Varovane podatke morajo hraniti, dokler se jih ne razreže ali uniči na drugačen varen način.

24. člen

Kadar uporabnik prenaša varovane podatke MOL v tujo državo, morajo biti shranjeni v nedosegljivi obliki, kot so šifrirane datoteke na prenosnih medijih ali pa morajo biti nenehoma pod nadzorom uporabnika.

25. člen

Varovani podatki MOL se ne uporabljajo ali kakor koli drugače izpostavljajo v restavracijah, na letalih, vlakih ali katerikoli drugih javnih krajih, kjer jih lahko prestrežejo nepooblaščen osebe. Med prenašanjem morajo ostati pod nadzorom uporabnika. Takšne informacije se ne sme puščati v nenadzorovanem vozilu, hotelski sobi ali drugi pisarni, tudi če sta vozilo ali soba zaklenjena.

26. člen

Uporabniki računalnikov in mobilnih naprav, ki vsebujejo varovane podatke MOL, te opreme ne smejo oddati v letališke prtljažne sisteme. Ta oprema mora ostati pod nadzorom uporabnika kot osebna prtljaga.

IX. KONČNI DOLOČBI

27. člen

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o uporabi računalniške in komunikacijske opreme pri delu na daljavo št. 386-1/2010-3 z dne 21. 1. 2010.

28. člen

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

Številka: 386-1/2010-22

Datum:

24-04-2018

Župan
Mestne občine Ljubljana
Zoran Jankovič

