

Na podlagi 16. člena v zvezi s 5. členom Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23), 51. in 89. člena Statuta Mestne občine Ljubljana (Uradni list RS, št. 31/21 – uradno prečiščeno besedilo) in 4. člena Odredbe o informacijski varnostni politiki št. 386-1/2024-1 z dne 11. 10. 2024 izdajam

P R A V I L N I K **O UPORABI ZASEBNE INFORMACIJSKE OPREME ZA SLUŽBENE NAMENE**

I. SPLOŠNE DOLOČBE

1. člen

Ta pravilnik z namenom zaščite podatkov in informacijskih storitev v lasti in upravljanju Mestne uprave Mestne občine Ljubljana (v nadaljnjem besedilu: MU MOL) določa informacijsko-varnostna pravila uporabe zasebne informacijske opreme za službene namene.

Uporaba zasebne informacijske opreme za službene namene po tem pravilniku je vsak uporabniški ali administrativni dostop do informacijskih storitev, ki so v upravljanju MU MOL (v nadaljnjem besedilu: zasebni dostop), pri katerem se uporabljajo informacijska sredstva, ki niso pod neposrednim upravljanjem MU MOL (v nadaljnjem besedilu: zasebna informacijska naprava).

Ta pravilnik se nanaša na lastnike zasebnih informacijskih naprav, ki le-te uporabljajo za zasebni dostop in so zaposleni v Mestni občini Ljubljana ali so zunanji pogodbeni izvajalci, ki vzdržujejo informacijska sredstva MU MOL, in ki pri tem uporabljajo zasebni dostop za poslovne potrebe MU MOL (v nadaljnjem besedilu: uporabnik), ter uslužbenke Službe za digitalizacijo (v nadaljnjem besedilu: SDIGI), ki administrativno-tehnično upravljajo s podatki in informacijskimi storitvami MU MOL.

2. člen

Pravilnik s ciljem obvladovanja ključnih tveganj v primeru uporabe zasebne informacijske naprave za zasebni dostop določa:

1. odobritev uporabe zasebne informacijske naprave za zasebni dostop s strani SDIGI ter operativne postopke nadzora uporabe s strani SDIGI;
2. seznanitev s tveganji in pravilno uporabo zasebne informacijske naprave za zasebni dostop, ki vključuje:
 - seznanitev z internimi akti, tj. odredbo, ki ureja informacijsko varnostno politiko, in pravilniki, ki urejajo upravljanje z informacijsko varnostjo, v MOL;
 - sprejemljivost in ustreznost uporabljane zasebne informacijske naprave, ki ni pod neposrednim nadzorom SDIGI;
 - ustreznost stanja operacijskega sistema in protivirusne zaščite in pravila osebnega profila za namene zasebnega dostopa;
 - razmejitev lastninske odgovornosti in vzdrževanja zasebne informacijske naprave;
 - način evidentiranja uporabnikov in zasebne informacijske naprave ter storitev v uporabi v primeru prihoda v MU MOL, prehoda med delovnimi enotami, odhoda iz MU MOL;
 - seznanitev s pravico SDIGI do oddaljenega izbrisa podatkov na napravi prek MDM sistema v upravljanju SDIGI v primeru kraje ali prekinitve zaposlitve v MU MOL;
 - seznanitev z obsegom dovoljenih aplikativnih funkcionalnosti, omejitve prenosa podatkov na zasebno informacijsko napravo in hramba gesel MU MOL storitev;
3. uporabo zasebne informacijske naprave za povezovanje prek kriptiranega kanala navideznega zasebnega omrežja (VPN) na delovno postajo zaposlenega.

II. ODOBRITEV UPORABE ZASEBNE INFORMACIJSKE NAPRAVE ZA ZASEBNI DOSTOP IN OPERATIVNI POSTOPKI NADZORA S STRANI SDIGI

3. člen

Zasebno informacijsko napravo je dovoljeno uporabljati za zasebni dostop na podlagi predhodne pisne odobritve SDIGI in na podlagi izjave lastnika zasebne informacijske naprave iz tretjega odstavka 4. člena tega pravilnika.

Ne glede na prejšnji odstavek se zasebne informacijske naprave, ki ustrezajo tehnološkim standardom in zmogljivostim informacijskih sistemov, kot jih predpiše, preveri in potrdi SDIGI, s katerimi se povezujejo, in ne zahtevajo dodatnih ali posebnih virov za namestitve in upravljanje, lahko izjemoma uporabljajo za zasebni dostop, če so upoštevana določila tega pravilnika in uporaba take informacijske naprave po presoji SDIGI ne povečuje tveganja informacijske varnosti.

Način povezovanja zasebne informacijske naprave z informacijskimi storitvami MU MOL za namene zasebnega dostopa zagotovi SDIGI. SDIGI vodi evidenco zasebnih informacijskih naprav za zasebni dostop, za katere je odobril zasebni dostop, ki vključuje podatke o uporabnikih zasebnega dostopa in storitvah iz seznama sredstev in pravic, ki ga vodi SDIGI, za katera je bil dostop odobren. Zasebno informacijsko napravo na podlagi obveznega predhodnega soglasja uporabnika lahko SDIGI doda v sistem za oddaljeno upravljanje in nadzor. SDIGI za storitve, ki se uporabljajo prek zasebnega dostopa, zagotovi kriptirano izmenjavo podatkov.

SDIGI izda in redno posodablja seznam tehničnih pogojev za odobritev zasebnega dostopa za zasebne informacijske naprave, ki vključuje seznam dovoljenih naprav in konfiguracij ter opisuje splošni postopek odobritve zasebnega dostopa, upošteva specifično vrsto naprave. Med tehničnimi pogoji za odobritev zasebnega dostopa mora biti predpisana tudi uporaba programske opreme za zaščito mobilne ali prenosne zasebne informacijske naprave. SDIGI opredeli uporabo samo preverjenih in vnaprej odobrenih aplikacij in programske opreme ter omejitve glede nameščanja aplikacij z neuradnih programskih tržnic v okviru uporabniškega računa za zasebni dostop v MU MOL na zasebni informacijski napravi.

SDIGI lahko od uporabnika zahteva posredovanje stanja konfiguracije. V primeru ugotovljenih neskladnosti uporabnika opozori in pozove k posodobitvi. SDIGI v primeru neupoštevanja določb tega odstavka uporabniku onemogoči rabo storitve.

Uporaba zasebne informacijske naprave za zasebni dostop je nadzorovana s strani SDIGI. Če SDIGI v omrežju zazna nedovoljeno napravo, zasebno informacijsko napravo odstrani ali jo onemogoči, dogodek pa se obravnava kot varnostni incident.

III. SEZNANITEV S TVEGANJI IN PRAVILNA UPORABA ZASEBNE INFORMACIJSKE NAPRAVE ZA ZASEBNI DOSTOP

4. člen

SDIGI zagotovi informativno gradivo za seznanitev uporabnikov s tveganji in pravilno uporabo zasebne informacijske naprave za zasebni dostop.

Uporabnik zasebne informacijske naprave, ki se uporablja za zasebni dostop, mora upoštevati določbe internih aktov, tj. odredbe, ki ureja informacijsko varnostno politiko v MOL, in pravilnikov, ki urejajo upravljanje z informacijsko varnostjo v MOL.

Uporabnik pred začetkom uporabe zasebne informacijske naprave za zasebni dostop podpiše izjavo, s katero dovoljuje vključitev naprave v sistem oddaljenega upravljanja in nadzora MU MOL in izbris podatkov MOL MU v primeru izgube naprave ali prekinitve zaposlitve.

Uporabnik mora zasebno informacijsko napravo redno varnostno in antivirusno posodabljati. SDIGI lahko predpiše sprejemljivo konfiguracijo naprave, ki jo mora uporabnik samostojno namestiti in vzdrževati.

Uporabniški račun za osebno ali družinsko uporabo ter uporabniški račun za zasebni dostop in namenski administrativni račun, s katerim se zasebna informacijska naprava izključno upravlja, morajo biti ločeni. Navadni uporabniški računi ne smejo omogočati administrativnih funkcij.

Uporaba nezaklenjenih naprav ali nezaklepanje zaslona ter hranjenje gesel MOL uporabniških računov za hitrejšo aktivacijo spletne storitve MU MOL neposredno na zasebni informacijski napravi je prepovedana. Uporabniška gesla uporabniških računov na zasebni informacijski napravi za zasebni dostop morajo biti kompleksna in skladna z internim aktom, tj. pravilnikom, ki ureja upravljanje uporabniških računov.

V primeru mobilne naprave je zasebni dostop dovoljen le v okviru varne mape.

V primeru zaznanih zlonamernih varnostnih dogodkov na zasebni informacijski napravi uporabnik o tem takoj obvesti SDIGI.

Uporabnik je v obdobju uporabe zasebne informacijske naprave za zasebni dostop odgovoren za varovanje celovitosti in zaupnosti okolja konkretne informacijske storitve, ki mu je s strani MU MOL predana v uporabo. Tako storitev lahko uporablja le sam osebno in le za konkretne poslovne namene. Prepovedana je vsaka nenamenska ali zlonamerna raba storitve ali predaja poverilnice tretjim osebam za namene opravljanja aktivnosti v njegovem imenu.

Uporabniki brez predhodnega pisnega dovoljenja poslovnega skrbnika ne smejo izvažati podatkov ali dokumentarnega gradiva izven področja storitve, kjer se podatki oziroma tako gradivo izvorno hranijo. V primeru prenosa delovnih gradiv je uporabnik sam odgovoren za ažurnost in verodostojnost podatkov v takih, od vira hrambe odklopljenih – lokalnih verzij dokumentov. Lokalnih verzij dokumenta po prenosu ni dovoljeno lokalno urejati in nameščati na izvorno lokacijo, ker bi lahko prišlo do spremembe verzije na izvoru.

Podatke ali varnostno neoporečne dokumente lahko namešča le tisti uporabnik, ki ima za to dodeljene pravice.

IV. PRAVILA POVEZOVANJA PREK KRIPTIRANEGA KANALA NAVIDEZNEGA ZASEBNEGA OMREŽJA (VPN) NA MU MOL DELOVNO POSTAJO ZAPOSLENEGA

5. člen

SDIGI v primeru izrednih razmer zagotovi pogoje za vzpostavitev varnega namenskega kriptiranega kanala za namene neposrednega imenskega povezovanja zasebne informacijske naprave uporabnika z oddaljenim računalnikom - informacijsko napravo v lasti MU MOL in upravljanju SDIGI, ki jo uporablja zaposleni v Mestni občini Ljubljana. Pogoji iz tega odstavka vključujejo:

- sistemsko storitev za vzpostavitev kriptiranega kanala na strani omrežja MU MOL;
- zagotovitev programske opreme za vzdrževanje namenskega kriptiranega kanala in navodil za namestitve;
- zagotovitev osebnega certifikata za dodatno raven varovanja, ki ga uporabnik namesti na zasebni informacijski napravi in navodila za namestitve.

Za zasebni dostop, vzpostavljen na podlagi prejšnjega odstavka, se uporabljajo določbe 3. in 4. člena tega pravilnika, razen obveznosti podpisa izjave uporabnika iz tretjega odstavka 4. člena tega pravilnika. Vse poslovne operacije in hramba podatkov ter vse varnostne kontrole se v tem primeru izvajajo skladno z internim aktom, tj. odredbo, ki ureja informacijsko varnostno politiko v MOL.



V. KONČNA DOLOČBA

6. člen

Ta pravilnik začne veljati naslednji dan po objavi na intranetni strani Mestne občine Ljubljana.

Številka: 386-1/2024-3

Datum: 11-10-2024

Župan
Mestne občine Ljubljana
Zoran Janković

