Pravilnik o dodeljevanju in nadzoru uporabniških dostopov

Zgodovina sprememb:

Verzija	Datum	Številka dokumenta
1	21.9.2011	007-47/2011/7
2	31.1.2013	007-47/2011/15
3	19.5.2014	007-47/2011/24
4	29.11.2017	007-47/2017/6
5	18.10.2018	007-47/2017/21

Na podlagi drugega odstavka 42. člena Zakona o državni statistiki (Ur. list RS, št. 45/1995, 9/2001) generalna direktorica Statističnega urada Republike Slovenije izdaja naslednji

Pravilnik o dodeljevanju in nadzoru uporabniških dostopov

1 SPLOŠNO

1.1 Namen

Pravilnik določa postopke dodeljevanja, spreminjanja in odvzemanja uporabniških dostopov do informacijskih virov Statističnega urada Republike Slovenije (v nadaljevanju: SURS) in s tem do podatkov, ki se v njih nahajajo ter opredeljuje kontrole, povezane z ugotavljanjem istovetnosti uporabnika in sledenjem njegovih aktivnosti v informacijskem sistemu.

1.2 Cilj

Cilj pravilnika je zmanjševanje tveganja nepooblaščenega dostopa do podatkov in s tem varovanje načela zaupnosti, to je, da so podatki dostopni samo pooblaščenim uporabnikom.

2 NAČRTOVANJE UPORABNIŠKIH VLOG IN PRAVIC

Pravice uporabnikov informacijskega sistema, s pomočjo katerih se omejuje dostop do podatkov posameznih informacijskih virov SURS, predstavljajo enega ključnih načinov zagotavljanja varnosti podatkov v informacijskem sistemu. Z dodeljevanjem ustreznih uporabniških pravic in vlog zagotovimo, da so spoštovana naslednja načela:

- načelo dodeljevanja uporabniškega dostopa samo tistim uporabnikom, ki pri svojem delu tak dostop nujno potrebujejo;
- načelo najmanjšega možnega dostopa do podatkov (angl. »need-to-know principle«);
- načelo ločevanja dolžnosti v tistih organizacijskih procesih, kjer je to potrebno.

Že ob samem razvoju ali prvi uvedbi programske rešitve je potrebno uporabniške pravice in vloge podrobno načrtovati.

Vsi podatki, ki so v skladu s Pravilnikom o klasifikaciji informacij opredeljeni kot občutljivi ali interni, se morajo hraniti in obdelovati v varovanih okoljih, ki omogočajo nadzor in omejevanje uporabniških dostopov. Hramba takšnih podatkov na lokalnih diskih delovnih postaj ni dovoljena.

SURS za namen upravljanja z uporabniškimi dostopi uporablja informacijski sistem za upravljanje z dostopi, ki zajema vse informacijske vire SURS in njihove skrbnike. Informacijski sistem za upravljanje z dostopi se uporablja v skladu z uporabniškimi navodili.

3 POSTOPEK DODELJEVANJA, SPREMINJANJA IN ODVZEMANJA PRAVIC

Za zaposlene, dijake in študente ter druge osebe, ki opravljajo delo na SURS in imajo dostop do informacijskega sistema SURS, se za vsak informacijski vir izvaja postopek dodeljevanja dostopa preko informacijskega sistema za upravljanje z dostopi.

Za namene upravljanja z uporabniškimi dostopi mora služba, pristojna za kadrovske in pravne zadeve vse spremembe v delovnih in pogodbenih razmerjih takoj zabeležiti v informacijski sistem za upravljanje z dostopi. Na podlagi vnesenih sprememb se samodejno generirajo obvestila za tehnične skrbnike, ki morajo na podlagi obvestil ustrezno ukrepati. Vse odsotnosti, daljše od treh mesecev, se

smatrajo kot začasno odvzemanje pravic – tem uporabnikom se uporabniški račun blokira, uporabniške pravice pa ne spreminjajo.

Uporabniški dostopi se dodeljujejo, spreminjajo in odvzemajo po naslednjem postopku:

- vsebinski skrbnik informacijskega vira na podlagi zahtev, ki jih prejme od vodij notranjih organizacijskih enot kreira zahtevo za dodelitev, spremembo ali odvzem dostopa preko informacijskega sistema za upravljanje dostopov. Zahteva se samodejno posreduje tehničnem skrbniku v realizacijo in v vednost vodji sektorja/službe, v katerega področje sodi informacijski vir. V kolikor gre za dostop do zbirke osebnih podatkov se zahteva avtomatsko posreduje v potrditev generalnemu direktorju.
- tehnični skrbniki informacijskih virov na podlagi zahtevka vsebinskega skrbnika poskrbijo za njegovo realizacijo in le to potrdijo v informacijskem sistemu za upravljanje dostopov.

Za uporabnike podatkov za znanstvenoraziskovalne namene ter v izjemnih primerih se z namenom preprečevanja nepooblaščenega dostopa do podatkov za vsak informacijski vir izvaja naslednji postopek dodeljevanja dostopa, ki uporabniku omogoči dostop do informacijskega vira in s tem podatkov:

- vsebinski skrbnik informacijskega vira na podlagi zahtev kreira elektronsko zahtevo za dodelitev, odvzem ali spremembo dostopa in jo zabeleži v zbirko dokumentarnega gradiva (in informacijo o zahtevi posreduje tehničnemu skrbniku ter v vednost vodji sektorja oz. službe, v katerega področje sodi informacijski vir;
- elektronska zahteva mora vključevati:
  - ✓ informacijske vire, do katerih naj bi imel uporabnik dostop in vrsto dostopa (branje, pisanje, spreminjanje ipd.);
  - ✓ predlog o trajanju ali ukinitvi dostopa;
- tehnični skrbniki informacijskih virov na podlagi zahtevka vsebinskega skrbnika poskrbijo za njegovo realizacijo.

Dodeljevanje, spreminjanje in odvzemanje uporabniških dostopov do zbirk osebnih podatkov poteka v skladu z 9. in 9.a členom Pravilnika o varstvu podatkov zbranih s programom statističnih raziskovanj na Statističnem uradu Republike Slovenije in v skladu z 4.a in 4.b členom Pravilnika o varstvu osebnih podatkov zaposlenih.

SURS vodi centralno evidenco upravljanja z uporabniškimi dostopi. Evidenca vsebuje podatke o informacijskih virih, njihovih skrbnikih, o vseh dostopih do informacijskih virov (kdo ima dostop do česa, kakšen dostop, kdo je zahtevek oddal, kdo odobril, kdo realiziral, čas trajanja dostopa). Evidenca se za zaposlene, dijake in študente ter druge osebe, ki opravljajo delo na SURS in imajo dostop do informacijskega sistema SURS vodi v sklopu informacijske rešitve za upravljanje dostopov. Za uporabnike podatkov za znanstvenoraziskovalne namene ter izjemne primere se evidenca upravljanja z uporabniškimi dostopi vodi v zbirki dokumentarnega gradiva.

4 NADZOR NAD UPORABNIŠKIMI DOSTOPI

Uporabnik mora skrbno varovati gesla, pametne kartice, certifikate za dostop do informacijskih virov tako, da se ne odtujijo ali zlorabijo. Vsak sum zlorabe ali odtujitve je treba takoj prijaviti sistemsko tehnični podpori.

4.1 Struktura uporabniških imen

Uporabniška imena morajo biti enotno strukturirana po vzorcu: PRIIMEKX (kjer je X prva črka imena, če druga oseba s tem priimkom že ima uporabniško ime v informacijskem sistemu). Pri vseh uporabniških imenih je potrebno zagotoviti, da so enostavno povezljiva z imenom in priimkom uporabnika.

Opredeljevanje in uporaba skupinskih uporabniških imen je dovoljeno samo, ko je mogoče enolično določiti končnega uporabnika.

Sistemska uporabniška imena so dovoljena le takrat, kadar so nujno potrebna za delovanje informacijskega sistema in se jih ne sme uporabljati za dostop do podatkov. Razkrivanje uporabniških imen in gesel ni dovoljeno. Prijava uporabnika v informacijski sistem z uporabniškim imenom, ki ni bilo dodeljeno temu uporabniku, ni dovoljeno.

4.2. Politika gesel

Politika gesel se izvaja z namenom zagotavljati kakovost gesel in njihovo redno menjavo, kar zmanjšuje tveganje nepooblaščenega dostopa oz. omejuje časovno daljše zlorabe. V ta namen mora biti politika gesel v domeni in drugih sistemih (kjer je to mogoče) nastavljena na minimalno naslednje nastavitve:

- onemogočena uporaba zadnjih 5 gesel;
- geslo je potrebno zamenjati vsakih 180 dni (izjemoma ne velja za sistemske račune, ki se ne uporabljajo za prijavo uporabnikov v sistem);
- ne glede na določbo prejšnje alineje lahko neposredni vodja ali njemu hierarhično nadrejeni ob ustrezni obrazložitvi zahteva takojšnjo spremembo uporabniških gesel posameznega uporabnika;
- geslo je mogoče zamenjati največ enkrat na dan;
- geslo mora biti dolgo vsaj 12 znakov;
- geslo mora biti kompleksno – vsebovati mora črke in druge alfanumerične znake;
- uporabniški račun se mora zakleniti po največ 5 neuspešnih poizkusih prijave;
- števec neuspešnih poizkusov prijave se resetira 30 minut po zadnji neuspešni prijavi;
- uporabniški račun se v primeru zaklenitve odklene po 30 minutah.

4.3. Politika administratorskih računov

Administratorski računi so dodeljeni izključno tehničnim skrbnikom posameznih delov informacijskega sistema (v nadaljevanju: sistemski informacijski viri) in pooblaščenim uporabnikom, ki lokalne administratorske račune potrebujejo za upravljanje sistemskih informacijskih virov ali delovnih postaj. Administratorski računi so predmet enakih določil politike nadzora nad uporabniškimi dostopi kot vsi ostali uporabniški računi, poleg teh pa zanje veljajo tudi določila v nadaljevanju.

Dodelitev lokalnih administratorskih računov delovnih postaj potrjuje skrbnik informacijske varnosti, ki vodi evidenco lokalnih administratorskih računov. Zahtevo za dodelitev lokalnega administratorskega računa delovne postaje kreira vodja zaposlenega, ki za učinkovito opravljanje dela potrebuje lokalni administratorski račun. Zahtevo z utemeljitvijo naslovi na skrbnika informacijske varnosti. V kolikor je utemeljitev upravičena, skrbnik informacijske varnosti posreduje zahtevek za dodelitev lokalnega administratorskega računa tehničnem skrbniku delovnih postaj, ki zahtevek realizira. Uporabniki lokalnih administratorskih računov morajo uporabljati dva uporabniška računa – enega, s katerim se prijavljajo na svojo delovno postajo kot običajen uporabnik in enega, ki ga uporabljajo za potrebe administracije. Ob uporabi lokalnega administratorskega računa morajo skrbeti za dokumentiranje vseh sprememb.

Zahtevo za dodelitev lokalnih administratorskih računov na posameznih sistemskih informacijskih virih kreira vsebinski skrbnik posameznega sistemskega informacijskega vira, realizira pa jo tehnični skrbnik. V kolikor se sistemski informacijski vir uporablja za obdelavo osebnih podatkov, se zahteva avtomatsko posreduje v potrditev generalnemu direktorju.

Na sistemskih informacijskih virih mora biti dokumentirano posebno administratorsko uporabniško ime in geslo za upravljanje tega vira. Dostop do tega imena in gesla se sme uporabiti le v primeru, ko to eksplicitno odobri generalni direktor. Uporaba, blokiranje ali izbris tega administratorskega uporabniškega imena brez ustrezne odobritve se smatra kot hujša kršitev delovnih obveznosti. Geslo za dostop do posebnega administratorskega računa se opredeli tako, da ga opredelita 2 osebi, od katerih

vsaka pozna le svoj del gesla oziroma na drug, s stališča informacijske varnosti, ustrezen način. Geslo za vsak sestavni del informacijskega sistema posebej se zapečati v ovojnico skupaj z dokumentom »Gesla sistemskih informacijskih virov«, ki se deponira v ognjevarno omaro, do katere imajo dostop le pooblaščene osebe v izrednih okoliščinah, ko je potrebno ravnati v skladu s pravilnikom o neprekinjenem delovanju. Vsaka uporaba vsebine zapečatene ovojnice se dokumentira. O uporabi vsebine zapečatene ovojnice se obvesti skrbnika informacijske varnosti.

Dokument »Gesla sistemskih informacijskih virov« vsebuje predvsem naslednje podatke:

- Naziv naprave in/ali aplikacije:
- Inventarna številka naprave:
- Lokacija naprave:
- Tehnični skrbnik:
- Datum:
- Podpis:
- Geslo:
- Navodila in opozorila za ravnanje z geslom in za zagon dotične naprave:

Na zapečateno ovojnico se zapišejo naslednji podatki:

- Naziv naprave oziroma aplikacije:
- Inventarna številka naprave:
- Lokacija naprave oziroma aplikacije:
- Tehnični skrbnik:
- Datum:
- Podpis:

4.4 Upravljanje infrastrukture javnih ključev

Za avtentikacijo uporabnikov SURS v nekaterih primerih uporablja infrastrukturo javnih ključev (Public key infrastructure - PKI). Pri upravljanju z infrastrukturo javnih ključev mora tehnični skrbnik PKI zagotoviti:

- ažurno evidenco imetnikov ključev;
- definirana pravila za kreiranje, spremembe ter izbris ključev;
- orodja in navodila za varno generiranje ključev za uporabnike;
- tehnično dokumentacijo z navodili za upravljanje sistemskega informacijskega vira v skladu z Pravilnikom o upravljanju informacijskega sistema;
- hrambo ključev in gesel v skladu s poglavjem 4.3 tega pravilnika.

4.5. Revizijske sledi

Za vse zbirke osebnih podatkov morajo biti vodene revizijske sledi v skladu z zakonom, ki ureja varstvo osebnih podatkov.

Za vse sistemske informacijske vire morajo biti vodene revizijske sledi z informacijami o vseh dogodkih, ki se izvajajo pod imenom administratorja, o neuspešni in uspešni prijavi uporabnika v sistem, o uspešnem in neuspešnem poizkusu dostopa do datotečnih storitev oziroma podatkov (npr. skupnih map), o vseh spremembah na uporabniških računih in o spremembah nastavitev.

Tehnični skrbniki ne smejo spreminjati vsebine dnevnikov oziroma jih brisati v nasprotju z zadnjim odstavkom te točke. Kršitev te določbe pomeni hujšo kršitev delovnih obveznosti.

Skrbnik informacijske varnosti mora redno (vsaj enkrat mesečno) pregledovati revizijske sledi ter preglede dokumentirati, zaznane varnostne dogodke pa obravnavati v skladu s Pravilnikom o postopkih za upravljanje varnostnih dogodkov.

V zvezi z sumom storitve kaznivega dejanja lahko pristojni preiskovalni organ pridobi podatke iz revizijske sledi skladno z zakonodajo.

Revizijske sledi se izbrišejo po treh mesecih, razen tistih, ki se nanašajo na zbirke osebnih podatkov. Tiste, ki se nanašajo na zbirke osebnih podatkov, se izbrišejo v skladu z zakonom, ki ureja varstvo osebnih podatkov.

4.6. Zaklepanje delovnih postaj in omejevanje uporabniških sej

Zaklepanje delovnih postaj je namenjeno zaščiti pred nepooblaščenim dostopom do informacijskih virov. Domenska politika se nastavi tako, da se delovna postaja samodejno zaklene po največ 20 minutah uporabniške neaktivnosti.

5 KONČNI DOLOČBI

Ta pravilnik začne veljati naslednji dan po objavi na internem portalu SURS.

Z dnem začetka veljavnosti tega pravilnika preneha veljati Pravilnik o dodeljevanju in nadzoru uporabniških dostopov št. 007-47/2017/6 z dne 29.11.2017.

Številka: 007-47/2017/21

Datum: 18. 10. 2018

Genovefa Ružić,
v. d. generalne direktorice