PATVIRTINTA
Kelmės rajono savivaldybės
administracijos direktoriaus
2016 m. d. įsakymu Nr.

KELMĖS RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kelmės rajono savivaldybės administracijos (toliau – Administracijos) informacinės sistemos naudotojų administravimo taisyklių (toliau – Taisyklės) tikslas – reglamentuoti naudotojų prieigos prie Administracijos informacinės sistemos (toliau – IS) valdymą siekiant užtikrinti elektroninės informacijos saugą.

2. Taisyklės taikomos Administracijos IS valdytojui ir tvarkytojams, duomenų valdymo ir saugos įgaliotiniui, visiems Administracijos IS naudotojams bei Administracijos IS administratoriui.

3. Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu, Nr. 1V-832, Bendruosiuose reikalavimuose organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintuose Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12), Administracijos informacinės dokumentų valdymo sistemos steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Administracijos direktoriaus 2015 m. birželio 19 d. įsakymu A-614, Administracijos IS duomenų saugos nuostatuose, patvirtintuose Administracijos direktoriaus 2015 m. rugpjūčio 7 d. įsakymu A-793 ir kituose teisės aktuose, reglamentuojančiuose saugų duomenų ir elektroninės informacijos tvarkymą, apibrėžtas sąvokas.

4. Prieinamumo prie elektroninės informacijos principas – naudotojas gali naudotis tik tomis IS posistemėmis, jose apdorojamais duomenimis ir bendraisiais resursais, prie kurių prieiga yra būtina pareigybės aprašyme, pareiginiuose nuostatuose numatytoms funkcijoms atlikti. Informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą informacinės sistemos administratoriaus paskyrą, kuria naudojantis negalima atlikti informacinės sistemos naudotojo funkcijos. Informacinių sistemų naudotojams negali būti suteikiamos informacinės sistemos administratoriaus teisės. Kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius).

II SKYRIUS
IS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

5. Naudotojų įgaliojimai renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant elektroninę informaciją yra nustatomi pagal pareigybės aprašyme reikalingą prieigos teisių lygmenį į IS.

6. Naudotojų teisės renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant elektroninę informaciją:

6.1. disponuoti vientisa, konfidencialia, prieinama informacija;

6.2. gauti visą informacijos pasiekiamumo lygį darbo dienomis darbo laiku;

6.3. reikalauti iš IS administratoriaus užtikrinti deramą duomenų apsaugos lygį;

6.4. gauti informaciją apie taikomas apsaugos priemones.

7. Naudotojų pareigos renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant elektroninę informaciją:

7.1. jungtis prie IS posistemių ir bendrųjų resursų įvedant tik asmeniškai suteiktus prisijungimo vardus ir slaptažodžius;

7.2. nesijungti prie IS posistemių ir bendrųjų resursų naudojantis kitam darbuotojui suteiktais prisijungimo vardais ir slaptažodžiais;

7.3. prisiimti atsakomybę už patikėtų tvarkomų duomenų rinkimą, įvedimą, naikinimą ir kt. (pagal pareigybės aprašymą ar pareiginius nuostatus);

7.4. nedelsiant pranešti IS administratoriui apie informacinės sistemos sutrikimus, neįprastą jų veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų naudotojų nederamus veiksmus;

7.5. neatskleisti, nelaikyti matomoje vietoje suteiktų prisijungimo vardų ir slaptažodžių;

7.6. prisiimti atsakomybę už tinkamą elektroninės informacijos tvarkymo programinių priemonių naudojimą ir techninių priemonių saugojimą;

7.7. elektroninės informacijos tvarkymo programinę ir techninę įrangą naudoti tik pareigybės aprašyme, pareiginiuose nuostatuose nurodytoms funkcijoms atlikti.

8. Administracijos IS administratoriaus (administratorių) įgaliojimai, teisės ir pareigos, tvarkant elektroninę informaciją:

8.1. atlieka funkcijas, numatytas Administracijos IS duomenų saugos nuostatuose;

8.2. vertina Administracijos IS naudotojams suteiktų teisių ir priskirtų funkcijų atitiktį;

8.3. vertina Administracijos IS naudotojų pasirengimą dirbti su Administracijos IS;

8.4. nagrinėja Administracijos IS naudotojų su Administracijos IS tvarkomais duomenimis atliktus veiksmus;

8.5. atlieka elektroninių incidentų tyrimą;

8.6. informuoja Administracijos IS duomenų saugos įgaliotinį apie Administracijos IS saugos dokumentų pažeidimus, galimos nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

8.7. vykdo Administracijos IS duomenų saugos įgaliotinio nurodymus ir pavedimus, susijusius su Administracijos IS elektroninės informacijos saugos užtikrinimu;

8.8. vykdo kitas tiesiogiai su Administracijos IS administravimu susijusias funkcijas.

9. Administracijos IS administratoriaus prieigos prie informacinės sistemos lygiai:

9.1. Administracijos IS administratorius:

9.1.1. administruoja visų Administracijos IS naudotojų prieigos teises prie Administracijos IS komponentų;

9.1.2. administruoja padalinio Administracijos IS naudotojų prieigos teises ir yra įgaliotas tvarkyti padalinio Administracijos IS duomenis;

9.1.3. vykdo techninę duomenų bazės priežiūrą ir neturi teisės tvarkyti duomenis kitaip, kaip tik atliekant susijusias administravimo užduotis.

III SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

10. Naudotojai su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, IS nuostatais, IS duomenų saugos nuostatais, Saugaus elektroninės informacijos tvarkymo taisyklėmis, Veiklos tęstinumo valdymo planu ir šiomis Taisyklėmis supažindinami pasirašytinai.

11. Naudotojo supažindinimas su saugos dokumentais turi būti vykdomas šiais atvejais:

11.1. prieš suteikiant naudotojui prieigą prie IS;

11.2. pakeitus duomenų saugos dokumentaciją;

11.3. periodiškai informacijos saugumo mokymų metu, ne rečiau kaip kartą per dvejus metus.

12. Supažindinimo su saugos dokumentais formą duomenų saugos įgaliotinis nustato savo nuožiūra, atsižvelgdamas į šias rekomendacijas:

12.1. jei supažindinamas vienas naudotojas, jam leidžiama su dokumentais susipažinti savarankiškai ir susitikimo metu įsitikinama, ar dokumentų turinys buvo tinkamai suprastas (užduodami klausimai);

12.2. jei supažindinama grupė naudotojų, surengiamas trumpas seminaras, kurio metu būtų pristatomi saugos dokumentai, apžvelgiamas jų turinys, užduodami klausimai naudotojams ir pateikiami paaiškinami;

12.3. saugos įgaliotinis elektroniniu paštu supažindina aptarnaujančius IS darbuotojus, naudotojų atstovus su IS saugos nuostatais, IS saugos dokumentais ir jų pakeitimais ne vėliau kaip kitą darbo dieną po jų įsigaliojimo.

IV SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

13. Už prieigos teisių prie IS suteikimą, pakeitimą ir panaikinimą yra atsakingas IS administratorius.

14. Naudotojų tapatybė informacinėje sistemoje nustatoma pagal unikalų vartotojo vardą, vartotojo sertifikatą.

15. Naudotojams prieigos prie IS posistemių teisės suteikiamos ar keičiamos Administracijos struktūrinio padalinio vadovui pateikus IS administratoriui prašymą įregistruoti darbuotoją IS naudotoju.

16. Naudotojams prieigos prie IS posistemių teisės suteikiamos per 2 darbo dienas nuo prašymo įregistruoti darbuotoją IS naudotoju pateikimo dienos.

17. Naudotojams prieigos prie IS posistemių teisės naikinamos, stabdomos ar keičiamos, kai Administracijos Teisės ir personalo skyrius pateikia Bendrajam priėmimo skyriui raštišką informaciją apie esminius valstybės tarnautojo ar darbuotojo statuso pakeitimus (atleidžiamas, perkeliamas, atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas, nebevykdo turėtų funkcijų ir pan.).

18. Administracijos IS naudotojo slaptažodžiui yra keliami šie reikalavimai:

18.1. slaptažodis turi būti iš ne trumpesnės kaip 8 simbolių kombinacijos, sudarytos iš raidžių, skaičių ir specialiųjų simbolių. Negalima naudoti lengvai nuspėjamų (pvz., vartotojo vardo, gimimo datos ir t.t.) slaptažodžių;

18.2. slaptažodis turi būti keičiamas ne rečiau kaip 1 kartą per tris mėnesius;

18.3. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius negali būti didesnis nei 5 kartai; neteisingai įvedus didžiausią leistiną skaičių, informacinė sistema užsirakina ir neleidžia informacinės sistemos naudotojui identifikuotis ne trumpiau nei 15 minučių;

18.4. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

18.5. keičiant slaptažodį, programinės įrangos priemonėmis neleidžiama sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

18.6. Administracijos IS naudotojas privalo saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;

18.7. Administracijos IS naudotojas, įtaręs, kad tretieji asmenys sužinojo slaptažodį, privalo nedelsdamas jį pakeisti.

19. Administracijos administratoriaus slaptažodžiams yra keliami šie papildomi reikalavimai:

19.1. Administracijos IS administratoriaus slaptažodis turi būti iš ne trumpesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

19.2. Administracijos IS administratoriaus slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

20. IS administratorius panaikina prieigos teisę prie konkrečios IS posistemės arba jos dalies, jeigu kyla įtarimų, kad naudotojas piktnaudžiauja suteiktomis prieigos teisėmis ir gali pažeisti IS arba joje apdorojamų duomenų saugumą. Administratorius kreipiasi į saugos įgaliotinį, kad gautų leidimą panaikinti naudotojo prieigos teises.

21. Vartotojams draudžiama prisijungti prie IS iš išorės, išskyrus atvejus, kai:

21.1. jungiamasi prie išorinės Administracijos interneto svetainės (prieiga neribojama);

21.2. IS administratorius gauna raštišką Administracijos vadovų leidimą administruoti IS.

22. Sistemos vartotojai turi turėti atitinkamą kvalifikaciją (kvalifikacijos kėlimo kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL vartotojo sertifikatas ar pan.) ir patirties (dirbant su tinkamomis operacinėmis sistemomis, taikomosiomis programomis ir pan.). Aukštesni nei Sistemos vartotojams reikalavimai turi būti nustatyti saugos įgaliotiniui ir administratoriams.

23. Sistemos vartotojai, pastebėję saugumo politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

24. Naudotojų atsakomybė reglamentuojama Lietuvos Respublikos įstatymų nustatyta tvarka.

_____

SUDERINTA
Vidaus reikalų ministerijos 2016 m. d. raštu Nr.