PATVIRTINTA
Nacionalinio maisto ir veterinarijos
rizikos vertinimo instituto direktoriaus
2022 m. vasario 3 d. įsakymu Nr. 1A-21

NACIONALINIO MAISTO IR VETERINARIJOS RIZIKOS VERTINIMO INSTITUTO INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinio maisto ir veterinarijos rizikos vertinimo instituto (toliau – NMVRVI) informacinės sistemos naudotojų administravimo taisyklės (toliau — Taisyklės) nustato NMVRVI informacinių sistemų (toliau — IS) naudotojų ir informacinių sistemų administratorių įgaliojimus, teises, pareigas ir saugaus duomenų teikimo IS naudotojams kontrolės tvarką, organizacinius ir techninius kibernetinio saugumo reikalavimus prieigos valdymui ir kontrolei.

2. Šios Taisyklės parengtos vadovaujantis Saugos dokumentų turinio gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimu aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informaciniu sistemų, registru ir kitu informacinių sistemų klasifikavimo gairių aprašo patvirtinimo", Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo", Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu ir kitais informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo " ir NMVRVI informacinės sistemos duomenų saugos nuostatais.

3. Taisyklėse vartojamos sąvokos atitinka Taisyklių 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Taisyklės taikomos visiems naudotojams, informacinių sistemų administratoriams ir saugos įgaliotiniui.

5. IS naudotojams prieiga prie IS duomenų suteikiama vadovaujantis šiais principais:

5.1. IS naudotojams prieiga turi būti suteikiama tik prie tų IS duomenų ir tik tokios apimties, kuri reikalinga IS naudotojo pareigybės aprašyme nurodytoms funkcijoms atlikti;

5.2. IS duomenis gali keisti (sukurti, papildyti ar panaikinti) tik tokią teisę turintys IS naudotojai;

5.3. prieiga prie IS duomenų ir teisę juos keisti suteikiama tik atlikus IS naudotojo identifikaciją ir patvirtinus jo tapatybę, asmens kodas negali būti naudojamas kaip IS naudotojo identifikatorius;

5.3.1. kiekvienas IS naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius);

5.4. IS naudotojams negali būti suteikiamos administratoriaus teisės.

II SKYRIUS
ADMINISTRATORIAUS IR NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. IS naudotojai turi teisę:

6.1. naudotis tik tomis IS funkcijomis ir IS duomenimis, prie kurių prieigą jiems suteikė administratorius;

6.2. gauti informaciją apie jų naudojamų IS duomenų apsaugos lygį ir taikomas apsaugos priemones, teikti pasiūlymus dėl papildomų apsaugos priemonių,

6.3. kreiptis į administratorių dėl neveikiančios ar netinkamai veikiančios IS.

7. IS naudotojai privalo:

7.1. naudoti IS duomenis tik tarnybinėms funkcijoms atlikti;

7.2. pranešti administratoriui apie IS saugos politikos įgyvendinamųjų teisės aktų pažeidimus, veiksmus, turinčius nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

7.3. užtikrinti jų naudojamų IS duomenų konfidencialumą ir vientisumą. savo veiksmais netrikdyti IS duomenų prieinamumo;

7.4. susipažinti su IS nuostatais, IS duomenų saugos nuostatais, NMVRVI informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėmis, IS informacinės sistemos veiklos tęstinumo valdymo planu, Šiomis Taisyklėmis ir kitais IS informacijos saugos įgyvendinamųjų teisės aktų reikalavimais ir jų laikytis;

7.5. pranešti administratoriui apie slaptažodžio užblokavimą ar užmiršimą;

7.6. pasitraukiant iš darbo vietos imtis priemonių, kad su IS tvarkomais duomenimis negalėtų susipažinti pašaliniai asmenys: atsijungti nuo IS, įjungti slaptažodžiu apsaugotą ekrano užsklandą.

8. IS naudotojui draudžiama:

8.1. leisti prisijungti prie IS ne IS naudotojui ar kitais nei Taisyklėse nustatytais būdais;

8.2. be priežiūros palikti kompiuteri, neatsijungus nuo IS;

8.3. platinti IS esančią informaciją, daryti jos kopijas ar kitu būdu dauginti.

9. Administratorius turi teisę:

9.1. matyti visų IS naudotojų identifikavimo ir suteiktų teisių duomenis;

9.2. matyti IS naudotojų su IS duomenimis atliktus redagavimo veiksmus;

9.3. atlikti užklausas IS pagal pasirinktus paieškos kriterijus;

9.4. pateikti paklausimus dėl IS naudotojų duomenų patikslinimo;

9.5. fiziškai prieiti prie techninės ir sisteminės programinės įrangos;

9.6. vykdyti IS techninės priežiūros funkcijas.

10. Administratorius privalo:

10.1. registruoti naujus IS naudotojus ir naikinti prisijungimo teises buvusiems IS naudotojams;

10.2. tvarkyti esamų IS naudotojų duomenis (pagal IS valdytojo pateiktus duomenis);

10.3. tvarkyti IS vidinius klasifikatorius, esančius IS klasifikatorių funkciniame modulyje;

10.4. konsultuoti IS naudotojus dėl IS veikimo ir kitais su IS susijusiais klausimais;

10.5. pagal kompetenciją užtikrinti nepertraukiamą IS techninės ir sisteminės programinės įrangos veikimą;

10.6. dalyvauti atliekant IS rizikos veiksnių įvertinimą ir rengiant IS rizikos veiksnių įvertinimo ataskaitą ir rizikos veiksniu įvertinimo ir rizikos veiksnių valdymo priemonių planą;

10.7. atlikti IS taikomų saugumo reikalavimų atitikties vertinimą.

11. Administratoriui draudžiama suteikti IS duomenų redagavimo teises ne IS naudotojams.

12. Administratoriaus funkcijos reglamentuotos IS saugos nuostatuose ir kituose IS saugos politikos įgyvendinamuosiuose teisės aktuose.

13. Saugos įgaliotinio funkcijos reglamentuotos IS saugos nuostatuose ir kituose IS saugos politikos įgyvendinamuosiuose teisės aktuose.

14. IS naudotojui, norint gauti prieigos prie IS duomenų teisę, IS naudotojo tiesioginis vadovas administratoriui teikia prašymą, kuriame nurodo būsimo IS naudotojo pareigas, vardą, pavardę ir poreikį prie kurių IS reikalingas prisijungimas (užpildoma KSF 8.3.5-1). Administratorius per 2 darbo dienas nuo prašymo gavimo dienos suteikia IS naudotojui prieigos prie IS duomenų teisę. Administratoriui teikiamas naudotojo prašymas turi būti vizuotas naudotojo tiesioginio vadovo.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO IS NAUDOTOJAMS KONTROLĖS TVARKA

15. Administratorius yra atsakingas už IS naudotojų registravimą, išregistravimą, prieigos prie IS teisių suteikimą ir panaikinimą.

16. Administratorius IS naudotojams suteikia unikalius prisijungimo prie IS vardą ir slaptažodį, kurį išsiunčia IS naudotojui elektroniniu paštu.

17. IS naudotojai prisijungti prie IS gali tik su administratoriaus suteiktais unikaliais vardais ir slaptažodžiais.

18. IS naudotojų prisijungimo prie IS vardai ir slaptažodžiai saugomi IS naudotojų prisijungimo vardų ir slaptažodžių elektroniniame žurnale saugykloje (KSF 8.3.5-4).

19. Prieigą prie saugyklos turi tik administratorius. Duomenys saugykloje yra šifruojami.

20. Prisijungti nuotoliniu būdu prie IS galima naudojant protokolą, skirtą duomenims šifruoti.

21. IS naudotojai, prisijungę prie IS, neturi teisės savarankiškai pasikeisti slaptažodžio.

22. IS naudotojo slaptažodžiui yra keliami reikalavimai:

22.1. slaptažodis turi būti iš ne trumpesnės kaip 8 simbolių kombinacijos, sudarytos iš didžiųjų ir mažųjų raidžių, skaičių ir (ar) specialiųjų simbolių,

22.2. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

22.3. keičiant slaptažodį nenaudoti slaptažodžio iš paskutiniųjų 3 buvusių slaptažodžių;

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

22.5. IS naudotojas, įtaręs, kad tretieji asmenys sužinojo slaptažodį, privalo nedelsdamas informuoti IS administratorių, inicijuodami slaptažodžio pakeitimą;

22.6. IS naudotojas neturi teisės užrašyto slaptažodžio palikti matomoje vietoje.

23. Administratoriaus slaptažodžiui yra keliami šie reikalavimai:

23.1. administratoriaus slaptažodis turi būti iš ne trumpesnis kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

23.2. keičiant slaptažodį nenaudoti slaptažodžio iš paskutiniųjų 3 buvusių slaptažodžių.

24. Administratorius, iš IS naudotojo tiesioginio vadovo gavęs prašymą apriboti IS naudotojo prieigos teises, nedelsdamas apriboja nurodyto IS naudotojo prieigą prie IS.

25. IS naudotojui teisė dirbti su konkrečia elektronine informacija yra sustabdoma, kai vyksta IS naudotojo veiklos tyrimas.

26. Kai IS naudotojas perkeliamas į kitas pareigas, jam suteiktos IS naudotojo teisės pakeičiamos atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

27. IS naudotojui teisę naudotis IS panaikinama arba sustabdoma:

27.1. pasibaigus tarnybos ar darbo santykiams;

27.2. netekus teisės naudotis IS duomenimis;

27.3. nustačius neteisėtą IS naudotojo IS duomenų naudojimą.

28. Nuotolinis naudotojų, administratorių prisijungimas prie IS turi būti vykdomas naudojant patikimus elektroninės informacijos šifravimo protokolus.

_____