PATVIRTINTA
Vilniaus universiteto rektoriaus
2012 m. balandžio 18 d. įsakymu Nr. R-155
(Vilniaus universiteto rektoriaus
2018 m. spalio 26 d. įsakymo Nr. R-580
redakcija)

VIRTUALI ISTORINĖ LIETUVA: LDK INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Virtuali istorinė Lietuva: LDK informacinės sistemos naudotojų administravimo taisyklės (toliau – Taisyklės) nustato Virtuali istorinė Lietuva: LDK informacinės sistemos (toliau – informacinė sistema) naudotojų administravimo tvarką.

2. Taisyklės parengtos vadovaujantis Bendruoju elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu, Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ Virtuali istorinė Lietuva: LDK informacinės sistemos nuostatais (toliau – Informacinės sistemos nuostatai) ir Virtuali istorinė Lietuva: LDK duomenų saugos nuostatais (toliau – Informacinės sistemos duomenų saugos nuostatai), patvirtintais Vilniaus universiteto rektoriaus 2012 m. balandžio 18 d. įsakymu Nr. R-155 „Dėl Virtuali istorinė Lietuva: LDK informacinės sistemos nuostatų ir Virtuali istorinė Lietuva: LDK informacinės sistemos duomenų saugos nuostatų patvirtinimo“, taip pat kitais teisės aktais ir standartais, reglamentuojančiais duomenų tvarkymo teisėtumą, tvarkytojų veiklą ir duomenų saugos valdymą.

3. Taisyklės taikomos informacinės sistemos valdytojui ir informacinės sistemos tvarkytojui, informacinės sistemos saugos įgaliotiniui, visiems informacinės sistemos naudotojams ir administratoriams.

4. Prieiga prie duomenų suteikiama vadovaujantis šiais principais:

4.1. Informacinės sistemos naudotojams ir administratoriams prieiga turi būti suteikiama tik prie tų duomenų ir tik tokia apimtimi, kuri reikalinga informacinės sistemos nuostatuose ir pareigybės aprašyme nurodytoms funkcijoms atlikti;

4.2. teisė keisti informacinėje sistemoje saugomus duomenis suteikiama tik atlikus informacinės sistemos naudotojo identifikaciją;

4.3. informacinės sistemos saugomus duomenis gali keisti (sukurti, papildyti ar panaikinti) tik tokius įgaliojimus turintys vidiniai informacinės sistemos naudotojai (ekspertai);

4.4. informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą informacinės sistemos administratoriaus paskyrą.

5. Taisyklėse vartojamos sąvokos atitinka Informacinės sistemos nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

II SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Informacinės sistemos naudotojų įgaliojimai, teisės ir pareigos, tvarkant elektroninę informaciją:

6.1. Informacinės sistemos naudotojai gali naudotis tik tomis informacinės sistemos funkcijomis ir informacinės sistemos tvarkomais duomenimis, prie kurių prieigą jiems suteikė informacinės sistemos administratorius, arba įgijo registruodamiesi informacinėje sistemoje savitarnos priemonėmis;

6.2. Informacinės sistemos naudotojai atsako už tinkamą savo registracijos paskyros asmens duomenų naudojimą ir saugojimą;

6.3. Informacinės sistemos naudotojams nėra suteikiama prieiga prie kitų informacinės sistemos naudotojų asmens duomenų;

6.4. Informacinės sistemos naudotojai turi teisę rinkti, tvarkyti, perduoti, įkelti, saugoti, naikinti ar kitaip naudoti elektroninę informaciją tik naudodamiesi savo paskyra; baigęs darbą, informacinės sistemos naudotojas turi užtikrinti, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo informacinės sistemos, uždaryti programinę įrangą, įjungti ekrano užsklandą su slaptažodžiu;

7. Informacinės sistemos naudotojai privalo:

7.1. savo veiksmais netrikdyti informacinės sistemos duomenų prieinamumo;

7.2. nesijungti prie informacinės sistemos naudojantis kitam informacinės sistemos naudotojui suteiktais prisijungimo vardais ir slaptažodžiais;

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

7.4. atsakingai vykdyti duomenų rinkimą, įvedimą, naikinimą ir kt.;

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

8. informacinės sistemos administratorių prieigos prie informacinės sistemos lygiai ir taikomi saugos reikalavimai:

8.1.1. administruoja visų informacinės sistemos naudotojų ir ekspertų prieigos teises prie informacinės sistemos komponentų;

8.1.2. mato informacinės sistemos naudotojų ir ekspertų su tvarkomais duomenimis atliktus veiksmus;

8.1.3. vykdo techninę duomenų bazės priežiūrą, duomenų archyvavimą, atkūrimą ir naikinimą bei neturi teisės tvarkyti duomenis kitaip, kaip tik atliekant susijusias administravimo užduotis.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

9. Informacinės sistemos naudotojai registruojasi informacinėje sistemoje savitarnos būdu.

10. Už informacinės sistemos ekspertų prieigos prie informacinės sistemos teisių suteikimą ir panaikinimą atsako paskirtas informacinės sistemos administratorius.

11. Esant poreikiui suteikti informacinės sistemos eksperto teises, informacinės sistemos administratorius, per 5 (penkias) darbo dienas nuo prašymo pateikimo dienos įvertinęs pateiktą informaciją, patvirtina papildomas informacinės sistemos paskyros teises arba informuoja naudotoją dėl kokių priežasčių prieiga nebuvo suteikta.

12. Informacinės sistemos naudotojo prieiga stabdoma praėjus 12 (dvylikai) mėnesių po paskutinio prisijungimo prie informacinės sistemos.

13. Informacinės sistemos naudotojų duomenys saugomi terminais, nustatytais Informacinės sistemos nuostatuose.

14. Prieiga prie informacinės sistemos taikomosios programinės įrangos ir ekspertinių duomenų tvarkyklės administravimo suteikiama raštišku prašymu, patvirtintu informacinės sistemos tvarkytojo ir informacinės sistemos duomenų valdymo įgaliotinio.

15. Esant informacinės sistemos tvarkytojo vadovo ir saugos įgaliotinio patvirtinimui, kitiems administratoriams teises informacinėje sistemoje suteikia ir panaikina informacinės sistemos tvarkytojo paskirtas administratorius.

16. Informacinės sistemos naudotojų tapatybei nustatyti turi būti suteikiamas prisijungimo prie informacinės sistemos vardas ir slaptažodis.

17. Registruojant naują informacinės sistemos naudotoją turi būti įrašoma tokia informacija, kad vienareikšmiškai būtų galima nustatyti asmens, besijungiančio prie informacinės sistemos, vardą ir pavardę.

18. Informacinės sistemos naudotojai turi teisę savarankiškai pasikeisti slaptažodį prisijungę prie informacinės sistemos.

19. Negalintis savarankiškai atgauti prieigos prie informacinės sistemos naudotojas turi kreiptis į informacinės sistemos administratorių, kuris nustatęs informacinės sistemos naudotojo tapatybę, suteikia informacinės sistemos naudotojui naują slaptažodį, kurį informacinės sistemos naudotojas, prisijungęs prie informacinės sistemos turi pasikeisti.

20. Informacinės sistemos naudotojo slaptažodžiui yra keliami šie reikalavimai:

20.1. slaptažodis turi būti iš ne trumpesnės kaip 8 simbolių kombinacijos, sudarytos iš raidžių, skaičių ir specialiųjų simbolių;

20.2. naudotojų slaptažodis turi būti keičiamas ne rečiau kaip kartą į metus;

20.3. 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;

20.4. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

20.5. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

20.6. informacinės sistemos naudotojai privalo saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;

20.7. informacinės naudotojas, įtaręs, kad tretieji asmenys sužinojo slaptažodį, privalo nedelsdamas jį pakeisti;

20.8. informacinės sistemos naudotojas neturi teisės užrašyto slaptažodžio palikti matomoje vietoje.

21. Informacinės sistemos administratorių slaptažodžiams yra keliami šie papildomi reikalavimai:

21.1. informacinės sistemos administratorių slaptažodis turi būti iš ne trumpesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

21.2. informacinės sistemos administratorių slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

22. informacinės sistemos administratorius, iš informacinės sistemos tvarkytojo gavęs rašytinį prašymą apriboti informacinės sistemos naudotojo prieigos teises, nedelsiant sustabdo nurodyto informacinių sistemų naudotojo prieigą prie informacinės sistemos.

23. Informacinės sistemos administratoriui teisė dirbti su konkrečia elektronine informacija yra ribojama sustabdant visas informacinės sistemos administratoriui suteiktas prieigos prie informacinės sistemos teises, kai vyksta informacinės sistemos administratoriaus veiklos tyrimas, informacinės sistemos administratorius neteikia informacijos apie saugą užtikrinančių sistemos komponentų būklę ar atsisako vykdyti saugos įgaliotinio nurodymus ir pavedimus.

24. Informacinės sistemos naudotojo prieiga naikinama:

24.1. Informacinės sistemos naudotojui nesutinkant ar atsisakius, kad būtų tvarkomi jo paskyros asmens duomenys;

24.2. nustačius elektroninės informacijos tvarkymo saugos reikalavimų pažeidimą ar neteisėtą informacinės sistemos duomenų tvarkymą.

25. Informacinės sistemos administratoriui teisė naudotis informacinės sistemos administratoriui skirta prieiga nedelsiant panaikinama:

25.1. pasibaigus tarnybos ar darbo santykiams;

25.2. nušalinus nuo pareigų;

25.3. nustačius neteisėtą informacinės sistemos naudotojo informacinės sistemos duomenų naudojimą.

26. Kai informacinės sistemos administratorius perkeliamas į kitas pareigas, jam suteiktos informacinės sistemos administratoriaus teisės pakeičiamos atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

27. Baigę duomenų tvarkymo darbus informacinės sistemos priemonėmis, informacinės sistemos administratoriai ir vidiniai naudotojai, turi atsijungti nuo informacinės sistemos.

28. Nuotolinis informacinės sistemos administratorių ir įgaliotų vidinių naudotojų prisijungimas prie informacinės sistemos tarnybinių stočių galimas tik naudojantis VPN tuneliu.

29. Prisijungimai ir (ar) bandymai prisijungi prie informacinės sistemos automatiniu būdu įrašomi informacinės sistemos duomenų bazės veiksmų žurnale, kuriame registruojami prisijungimo ir (ar) bandymo prisijungti data, laikas, prisijungimo trukmė, prisijungiančio informacinės sistemos naudotojo vardas ir kompiuterio, iš kurio prisijungiama IP adresas, informacinės sistemos funkcijos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai). Šie įrašai saugomi ne trumpiau kaip 1 metus.

_____