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 DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Virtuali istorinė Lietuva: LDK informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Virtuali istorinė Lietuva: LDK informacinės sistemos (toliau – informacinė sistema) elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir informacinės sistemos naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos informaciją, užtikrinti elektroninės informacijos prieinamumą ir vientisumą.

3. Saugos nuostatai parengti vadovaujantis Bendrųjų 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), 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“ ir informacinės sistemos nuostatais, 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.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos prieinamumo užtikrinimas;

4.2. elektroninės informacijos vientisumo užtikrinimas;

4.3. informacinės sistemos veiklos tęstinumas.

5. Valdytojo ir Tvarkytojo pavadinimai ir adresai:

5.1. informacinės sistemos valdytojas (toliau – Valdytojas) ir tvarkytojas (toliau – Tvarkytojas) yra Vilniaus universitetas (toliau – Universitetas), Universiteto g. 3, LT-01513, Vilnius.

5.2. Valdytojo funkcijas atlieka Universiteto Istorijos fakultetas, Universiteto g. 3, Vilnius.

5.3. Tvarkytojo funkcijas atlieka Universiteto Informacinių technologijų paslaugų centras, Saulėtekio al. 9, Vilnius.

6. Valdytojo funkcijos ir atsakomybė:

6.1. prižiūri, kaip laikomasi informacinės sistemos duomenų saugos reikalavimų;

6.2. rengia įsakymus dėl informacinės sistemos saugumo užtikrinimo, tikrina, kaip jie vykdomi;

6.3. atsako už informacinės sistemos saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

6.4. skiria duomenų valdymo įgaliotinį.

7. Tvarkytojo funkcijos ir atsakomybė:

7.1. užtikrina nepertraukiamą informacinės sistemos veikimą, elektroninės informacijos, esančios informacinėje sistemoje, saugą ir saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

7.2. teikia pasiūlymus Valdytojui, kaip tobulinti informacinės sistemos saugą;

7.3. užtikrina tinkamą Valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

7.4. skiria informacinės sistemos saugos įgaliotinį (toliau – saugos įgaliotinis);

7.5. skiria informacinės sistemos administratorių (toliau – administratorius) arba kelis administratorius, vykdančius atskiras informacinės sistemos administravimo funkcijas;

7.6. užtikrina informacinės sistemos sąveiką su kitomis informacinėmis sistemomis;

7.7. Tvarkytojo vadovas yra atsakingas už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politikos įgyvendinamuosiuose dokumentuose nustatyta tvarka.

8. Duomenų valdymo įgaliotinis, vadovaudamasis informacinių technologijų plėtros planu, kitais institucijos planavimo dokumentais:

8.1. įgyvendina informacinės sistemos plėtrą;

8.2. tiesiogiai prižiūri, kaip kuriama ir tvarkoma informacinė sistema, diegiama programinė įranga, panaudojamos investicijos;

8.3. rengia informacinės sistemos biudžetų projektus;

8.4. tiesiogiai prižiūri, kad informacija, duomenys, dokumentai ir (arba) jų kopijos būtų teikiami, skelbiami ir (arba) perduodami pagal teisės aktuose nustatytus reikalavimus;

8.5. teikia pasiūlymus dėl darbuotojų, kuriems pavesta tvarkyti informacinės sistemos duomenis, informaciją, dokumentus ir (arba) jų kopijas, teisių ir pareigų;

8.6. organizuoja informacinės sistemos turto inventorizacijas;

8.7. užtikrina informacinės sistemos naudotojų pasirengimą dirbti su informacine sistema;

8.8. atsako už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą;

8.9. atlieka kitas teisės aktuose nustatytas funkcijas.

9. Saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia Tvarkytojo vadovui pasiūlymus dėl:

9.1.1. administratoriaus (administratorių) paskyrimo;

9.1.2. informacinių technologijų saugos atitikties vertinimo Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka;

9.1.3. saugos dokumentų priėmimo, keitimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupės;

9.3. teikia administratoriui (administratoriams) privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo;

9.4. organizuoja informacinės sistemos rizikos įvertinimą;

9.5. periodiškai organizuoja administratorių mokymą elektroninės informacijos saugos klausimais;

9.6. atlieka kitas Valdytojo ir/ar Tvarkytojo vadovo pavestas ir kituose teisės aktuose jam priskirtas funkcijas.

10. Administratorius (administratorių) funkcijos:

10.1. užtikrina paskirtos informacinės sistemos infrastruktūros ir /arba taikomosios programinės įrangos veikimą;

10.2. administruoja informacinės sistemos ekspertų ir naudotojų prieigos teises;

10.3. analizuoja informacinės sistemos naudotojų ir ekspertų veiksmų registracijos žurnalų įrašus;

10.4. kuria ir atkuria atsargines informacinės sistemos kopijas;

10.5. rengia ir tikrina informacinės sistemos diegimo sąranką;

10.6. nustato pažeidžiamas informacinės sistemos vietas ir užtikrina savalaikį sistemos saugos spragų šalinimą;

10.7. atlieka su informacinės sistemos administravimu susijusias užklausas ir rengia naudojimo ataskaitas;

10.8. konsultuoja informacinės sistemos naudotojus dėl informacinės sistemos veikimo ir kitais su susijusiais klausimais;

10.9. atlieka visiškus ar dalinius duomenų atkūrimo bandymus iš atsarginių informacinės sistemos saugomų duomenų kopijų;

10.10. atlieka informacinės sistemos naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

10.11. informuoja saugos įgaliotinį apie saugos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

10.12. vykdo privalomus duomenų valdymo ir saugos įgaliotinio nurodymus;

10.13. atlieka kitas teisės aktuose nustatytas funkcijas.

11. Saugų informacinės sistemos duomenų tvarkymą reglamentuoja:

11.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

11.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

11.3. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas 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“ (toliau – Gairių aprašas);

11.4. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

11.5. Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymas Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.6. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką (toliau – saugos politika) ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą bei duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. Vadovaujantis Gairių aprašo 10 ir 12.4 punktų nuostatomis, informacinėje sistemoje tvarkoma elektroninė informacija pagal jos svarbą laikoma mažiausios svarbos elektronine informacija ir pagal joje apdorojamos elektroninės informacijos svarbą informacinė sistema priskiriama kitų, viešojo administravimo funkcijoms neskirtų informacinių išteklių, ketvirtos kategorijos informacinėms sistemoms.

13. Informacinėje sistemoje asmens duomenys tvarkomi tik vidaus administravimo reikmėms, naudotojų paskyroms administruoti.

14. Saugos įgaliotinis, vadovaudamasis metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja informacinės sistemos rizikos vertinimą. Prireikus, saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos vertinimą.

15. Informacinės sistemos rizikos vertinimas surašomas ataskaitoje, kuri pateikiama Valdytojo ir Tvarkytojo funkcijas atliekančių padalinių vadovams.

16. Informacinės sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

16.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

16.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

16.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

17. Informacinės sistemos rizikos vertinimo metu atliekami darbai:

17.1. įtakos informacinės sistemos veiklai vertinimas;

17.2. grėsmės ir pažeidimų analizė;

17.3. liekamosios rizikos vertinimas.

18. Atlikus rizikos įvertinimą, esant poreikiui, saugos įgaliotinis rengia ir teikia Valdytojui tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

19. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

19.1. liekamoji rizika turi būti sumažinama iki priimtino lygio;

19.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

19.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

20. atsižvelgdamas į informacinės sistemos rizikos įvertinimo ataskaitą, Valdytojas prireikus tvirtina informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis informacinės sistemos rizikos valdymo priemonėms įgyvendinti.

21. Siekiant užtikrinti informacinės sistemoms saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per du metus atlieka informacinės sistemos saugos atitikties vertinimą, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

22. Atlikus informacinės sistemos saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Valdytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Valdytojo vadovas.

23. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Programinės įrangos, skirtos informacinei sistemai nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

24.1. užtikrinama kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.);

24.2. nustačius pažeidžiamumą, apsaugai naudojama programinė įranga privalo būti atnaujinama nedelsiant;

25. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

25.1. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

25.2. naudojama tik legali programinė įranga;

25.3. programinė įranga yra nuolatos atnaujinama laikantis gamintojo reikalavimų;

25.4. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik administratoriai.

26. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. proxy) ir kt.) pagrindinės naudojimo nuostatos:

26.1. informacinės sistemos kompiuteriniai tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis;

26.2. visas informacinės sistemos duomenų srautas į ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenkėjiškos programinės įrangos;

26.3. Papildomos priemonės kompiuteriams ir mobiliems įrenginiams, kurie gali būti panaudoti nustatytoms administravimo funkcijoms atlikti ne Universiteto patalpose, nustatomos Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

27. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

27.1. nuotolinis prisijungimas prie informacinės sistemos galimas naudojantis „IPSec“ (angl. Internet Protocol Security) protokolų rinkiniu ir jungiantis kaip „IPSec“ programiniam klientui.

27.2. teikti elektroninę informaciją automatiniu būdu galima tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

28. Informacinės veiklos tęstinumo užtikrinimui elektroninė informacija yra periodiškai kopijuojama į rezervinių kopijų laikmenas kas 24 valandos ir laikmenos saugomos taip, kad avarijos atveju informacinę sistemą galima būtų atkurti taip, kad informacinės sistemos neveikimo laikotarpis būtų neilgesnis nei 24 valandos.

29. Informacinės sistemos prieinamumas per metus turi būti užtikrintas ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

30. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. saugos įgaliotinis privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

31. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumo srityje, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau nei vieni metai.

32. administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą. Administratorius privalo mokėti administruoti ir prižiūrėti duomenų bazes, būti susipažinęs su Saugos nuostatais ir kitais informacinės sistemos saugos politikos įgyvendinamaisiais teisės aktais.

33. Administratoriai privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, išmanyti informacinės sistemos komponentų administravimo ir priežiūros pagrindus, būti susipažinę su informacinės sistemos saugos dokumentais ir sutikę laikytis jų reikalavimų.

34. Informacinės sistemos vidiniai naudotojai turi:

34.1. turėti pagrindinius darbo su kompiuteriu įgūdžius;

34.2. mokėti tvarkyti elektroninius duomenis informacinės sistemos nuostatuose nustatytais tikslais;

34.3. būti susipažinę su informacinės sistemos saugos politiką įgyvendinančiais teisės aktais.

35. Informacinės sistemos naudotojų mokymų planavimą ir organizavimą bei naujų vidinių naudotojų supažindinimą su informacinės sistemos saugos reikalavimais darbo vietose vykdo administratorius.

36. Informacinės sistemos naudotojai ir administratoriai, pažeidę Saugos nuostatų ar kitų saugos politikos įgyvendinamųjų teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir Universiteto darbo tvarkos taisyklėse nustatyta tvarka.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Su Saugos nuostatais susipažįstama pasirašytinai arba elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

38. Saugos nuostatai ir kiti saugos politikos įgyvendinamieji teisės aktai skelbiami informacinės sistemos naudotojams pasiekiamoje interneto svetainėje.

39. Pakartotinai su saugos politiką reguliuojančiais teisės aktais informacinės sistemos naudotojai supažindinami esminiai pasikeitus informacijos saugą reguliuojantiems teisės aktams. Informacija apie saugos politikos įgyvendinamųjų teisės aktų pakeitimus siunčiama elektroniniu būdu.

_____