PATVIRTINTA
Vilniaus universiteto rektoriaus
2014 m. lapkričio 20 d. įsakymu Nr. R- 512

VILNIAUS UNIVERSITETO STUDIJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Vilniaus universiteto studijų informacinės sistemos (toliau – VUSIS) duomenų saugos nuostatų (toliau – VUSIS saugos nuostatai) tikslas – nustatyti VUSIS duomenų saugos procese dalyvaujančius subjektus ir apibrėžti jų funkcijas, įtvirtinti su studijų procesu Vilniaus universitete (toliau – Universitetas) susijusios elektroninės informacijos saugos valdymo nuostatas, nustatyti organizacinius ir techninius duomenų saugos reikalavimus, VUSIS naudotojų supažindinimo su VUSIS saugos dokumentais principus.
2. VUSIS saugos nuostatuose vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, vartojamas sąvokas.
3. Tvarkant VUSIS duomenis bei užtikrinant VUSIS duomenų saugą vadovaujamasi šiais Lietuvos Respublikos įstatymais ir kitais teisės aktais:
   3.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;
   3.2. Lietuvos Respublikos elektroninių ryšių įstatymu;
   3.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;
   3.4. Lietuvos Respublikos valstybės registrų įstatymu;
   3.5. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12);
   3.6. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
   3.7. Saugos dokumentų turinio aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
   3.8. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
   3.9. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 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“;
   3.10. Lietuvos standartais LST ISO/IEC 17799:2006 ir LST ISO/IEC 27002:2009, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais.
4. VUSIS saugos nuostatai apibrėžia VUSIS duomenų saugos politiką (toliau – saugos politika). VUSIS saugos politiką įgyvendina ir elektroninės informacijos saugą Universitete reglamentuoja šie dokumentai:
   4.1. Vilniaus universiteto studijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – VUSIS tvarkymo taisyklės);
   4.2. Vilniaus universiteto studijų informacinės sistemos veiklos tęstinumo valdymo planas (toliau – VUSIS valdymo planas);

4.3. Vilniaus universiteto studijų informacinės sistemos naudotojų administravimo taisyklės (toliau – VUSIS naudotojų administravimo taisyklės).

5. VUSIS saugos politika vykdoma šiomis prioritetinėmis kryptimis:

5.1. įgyvendinant VUSIS duomenų teikėjų teikiamų duomenų ir veiksmų su jais automatinį stebėjimą ir įrašų kaupimą;

5.2. įgyvendinant VUSIS naudotojams prieigos prie VUSIS duomenų automatinį teisių suteikimą, jų tapatumo identifikavimą ir veiksmų stebėjimą;

5.3. įgyvendinant VUSIS duomenų saugų kopijavimą, archyve esančių kopijų saugojimą;

5.4. įgyvendinant VUSIS duomenų saugą nuo žalingos programinės įrangos poveikio;

5.5. įrengiant VUSIS duomenims administruoti skirtas saugias patalpas ir kompiuterizuotas darbo vietas jose;

5.6. įgyvendinant VUSIS duomenims administruoti skirto personalo kvalifikacijos tobulinimo sistemą;

5.7. įgyvendinant VUSIS duomenų automatinį integralumą su kitomis informacinėmis sistemomis;

5.8. įgyvendinant VUSIS programinės, techninės įrangos saugą nuo nesankcionuoto poveikio joms ir (ar) jų modifikavimo;

5.9. įgyvendinant ryšių su VUSIS duomenų teikėjais, išorinėmis šalimis ir saugos specialistais jose palaikymą, plėtojimą;

5.10. įgyvendinant VUSIS saugos atitikties vertinimą.

6. **VUSIS valdytojas – Vilniaus universitetas,** adresas - Universiteto g. 3, LT-01513 Vilnius, kuris atsako už VUSIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą. Sistemos valdymo funkcijas Vilniaus universitete atlieka Studijų direkcija, kuri:

6.1. koordinuoja VUSIS saugos nuostatų, VUSIS saugos politiką įgyvendinančių teisės aktų rengimą ir kontroliuoja jų įgyvendinimą;

6.2. koordinuoja VUSIS funkcijų pokyčių planavimą;

6.3. koordinuoja elektroninės informacijos tvarkymo teisėtumo priežiūrą ir užtikrinimą;

6.4. koordinuoja VUSIS saugos politikos įgyvendinimą.

7. **VUSIS tvarkytojas** – Universiteto Informacinių technologijų taikymo centras (toliau – ITTC) (adresas - Saulėtekio al. 9, II jungiamieji rūmai, LT-10222, Vilnius), kuris atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka. VUSIS tvarkytojas:

7.1. užtikrina VUSIS saugos nuostatų ir teisės aktų, įgyvendinančių VUSIS saugos politiką, įgyvendinimą;

7.2. užtikrina VUSIS duomenų saugą;

7.3. įgyvendina VUSIS saugos nuostatuose, VUSIS saugos politiką įgyvendinančiuose teisės aktuose nustatytas VUSIS duomenų saugaus rinkimo, sisteminimo, saugojimo ir teikimo VUSIS duomenų gavėjams organizacines, technines ir kitas priemones;

7.4. teikia VUSIS valdytojui siūlymus dėl VUSIS saugos politikos įgyvendinimo plėtros, techninių, programinių priemonių įsigijimo, jų modernizavimo, priežiūros ir tobulinimo;

7.5. užtikrina VUSIS funkcijų pokyčių įgyvendinimą;

7.6. teisės aktų nustatyta tvarka teikia informaciją apie VUSIS saugos politikos įgyvendinimą;

7.7. skiria VUSIS pagrindinį ir duomenų bazių administratorius, paveda jiems vykdyti techninį VUSIS duomenų administravimą;

7.8. atlieka kitas norminiuose teisės aktuose, VUSIS saugos nuostatuose ir teisės aktuose, įgyvendinančiuose VUSIS saugos politiką, funkcijas.

8. **VUSIS pagrindinis administratorius** administruoja visų VUSIS naudotojų prieigos teises prie VUSIS programų. VUSIS pagrindinis administratorius:

8.1. yra įgaliotas tvarkyti visų Universiteto padalinių VUSIS duomenis;

8.2. pateikus prašymą, suteikia ir panaikina teises Universiteto padalinio vadovybės paskirtam VUSIS padalinio administratoriui;

8.3. palaiko ryšį su Universiteto kamieninių akademinių padalinių studijų administratoriais, nuolat keičiasi su jais informacija.

9. **VUSIS padalinio administratorius** administruoja padalinio VUSIS naudotojų prieigos teises prie programų. VUSIS padalinio administratorius:

9.1. yra įgaliotas tvarkyti padalinio VUSIS duomenis;

9.2. pateikus prašymą, suteikia teises Universiteto padalinio vadovybės paskirtam VUSIS padalinio administratoriui;

9.3. palaiko ryšį su padalinio studijų administratoriais, nuolat keičiasi su jais informacija.

10. **VUSIS duomenų bazės** (toliau – VUSIS DB) **administratorius** vykdo techninę VUSIS duomenų bazės priežiūrą. VUSIS DB administratorius:

10.1. užtikrina VUSIS DB saugumą;

10.2. vykdo VUSIS DB stebėseną;

10.3. prižiūri ir atnaujina VUSIS DB programinę įrangą.

11. **VUSIS administratoriai (visų tipų)**:

11.1. vykdo VUSIS duomenų teikėjų teikiamų duomenų administravimą (pagrindinis ir padalinių administratoriai);

11.2. vykdo VUSIS naudotojų veiksmų administravimą (pagrindinis, DB ir padalinių administratoriai);

11.3. vykdo VUSIS duomenų saugaus kopijavimo ir archyve esančių kopijų saugojimo administravimą (DB administratorius);

11.4. vykdo VUSIS duomenų apsaugos nuo jiems kenksmingos programinės įrangos poveikio administravimą (DB administratorius);

11.5. reaguoja į VUSIS elektroninės informacijos saugos incidentus;

11.6. vykdo visus VUSIS duomenų saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu, ir nuolat teikia duomenų saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

11.7. atlieka VUSIS tvarkytojo vadovo jam pavestas kitas su VUSIS saugos politika susijusias funkcijas (pagrindinis, DB ir padalinių administratoriai).

12. **VUSIS duomenų saugos įgaliotinis** įgyvendina elektroninės informacijos saugos politiką VUSIS. VUSIS duomenų saugos įgaliotinis:

12.1. teikia VUSIS valdytojui ir tvarkytojui siūlymus dėl VUSIS saugos nuostatų, VUSIS saugos politiką įgyvendinančių teisės aktų keitimo ir (ar) naujų teisės aktų priėmimo;

12.2. teikia VUSIS valdytojui siūlymus dėl VUSIS administratorių paskyrimo ir reikalavimų jiems nustatymo;

12.3. organizuoja VUSIS naudotojų mokymus duomenų saugos klausimais ir informuoja VUSIS naudotojus apie duomenų saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujiems darbuotojams ir kt.);

12.4. organizuoja VUSIS saugos atitikties ir rizikos vertinimą ir rengia VUSIS rizikos įvertinimo ataskaitą;

12.5. koordinuoja VUSIS duomenų saugos incidentų tyrimą VUSIS veiklos tęstinumo valdymo plane nustatyta tvarką;

12.6. ne rečiau kaip kartą per metus peržiūri VUSIS saugos nuostatus, VUSIS saugos politiką įgyvendinančius teisės aktus ir, esant reikalui, inicijuoja šių dokumentų pakeitimus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba institucijoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių;

12.7. atlieka kitas norminiuose teisės aktuose, VUSIS saugos nuostatuose ir teisės aktuose, įgyvendinančiuose VUSIS saugos politiką, funkcijas.

13. **VUSIS naudotojai** – autorizuoti vartotojai, turintys teisę naudotis VUSIS ištekliais savo funkcijoms atlikti. VUSIS naudotojai yra kelių lygių: Universiteto centrinės administracijos

darbuotojai, akademinių padalinių vadovai (aukštesnio lygio administratoriai), akademinių padalinių atsakingi darbuotojai (administratoriai), dėstytojai ir studentai.

14. VUSIS saugos nuostatai, VUSIS saugos politiką įgyvendinantys teisės aktai yra privalomi VUSIS valdytojui, VUSIS tvarkytojui, VUSIS pagrindiniam administratoriui, VUSIS padalinių administratoriams, VUSIS DB administratoriams, VUSIS duomenų saugos įgaliotiniui ir VUSIS naudotojams.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 4.3 punktu ir 4.3.1, 4.3.2, 4.3.3 ir 4.3.4 papunkčiais, VUSIS tvarkoma elektroninė informacija pagal jos svarbą laikoma žinybinės svarbos elektronine informacija. Vadovaujantis minėto aprašo 5.3 punktu, pagal joje apdorojamos elektroninės informacijos svarbos kategoriją VUSIS priskiriama trečiai informacinių sistemų kategorijai.

16. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12) 7.2 punktu, atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką VUSIS priskiriama antram saugumo lygiui.

17. VUSIS tvarkomi:

17.1. bendrieji studijuojančiųjų ir studijų duomenys, nurodyti VUSIS nuostatuose;

17.2. identifikaciniai asmens, įvedusio/koregavusio duomenis VUSIS, duomenys.

18. VUSIS duomenis VUSIS duomenų gavėjams teikia VUSIS tvarkytojas VUSIS nuostatų nustatytu būdu ir tvarka.

19. VUSIS duomenų aktualumas užtikrinamas VUSIS duomenų teikėjų automatiniu būdu kasdien teikiamais aktualiais duomenimis ir VUSIS posistemių integruota veikla.

20. VUSIS duomenų saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje (http://www.vrm.lt/Rizikos_analize.pdf), Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja VUSIS rizikos įvertinimą. Pasikeitus VUSIS funkcinei sandarai, atsiradus naujiems rizikos veiksniams, VUSIS tvarkytojo vadovo pavedimu VUSIS duomenų saugos įgaliotinis organizuoja neeilinį VUSIS rizikos įvertinimą.

21. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai VUSIS duomenims, programinei, techninei įrangai yra:

21.1. subjektyvūs netyčiniai veiksniai (duomenų tvarkymo klaidos, klaidingų duomenų teikimas, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos ir kita);

21.2. subjektyvūs tyčiniai veiksniai (nesankcionuotas naudojimasis informacine sistema siekiant gauti duomenų, duomenų keitimas, naikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, vagystės ir kita);

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

22. Rizikos veiksnių tikėtumui VUSIS duomenims, programinei, techninei įrangai įvertinti naudojama penkiabalė rizikos veiksnių tikėtumo vertinimo metodika:

22.1. nereikšmingas rizikos veiksnių tikėtumas – 1 balas;

22.2. mažas rizikos veiksnių tikėtumas – 2 balai;

22.3. vidutinis rizikos veiksnių tikėtumas – 3 balai;

22.4. didelis rizikos veiksnių tikėtumas – 4 balai;
22.5. labai didelis rizikos veiksnių tikėtumas – 5 balai.

23. VUSIS rizikos įvertinimo ataskaitą rengia VUSIS duomenų saugos įgaliotinis ir teikia ją tvirtinti VUSIS tvarkytojo vadovui.

24. Atlikus rizikos įvertinimą, esant reikalui, VUSIS duomenų saugos įgaliotinis rengia ir teikia VUSIS valdytojui tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. Siekiant užtikrinti VUSIS saugos nuostatuose ir kituose VUSIS saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, VUSIS duomenų saugos įgaliotinis kas dvejus metus organizuoja VUSIS saugos atitikties vertinimą, kurio metu:

24.1. įvertinama VUSIS saugos nuostatų ir VUSIS saugos politiką įgyvendinančių teisės aktų atitiktis realiai VUSIS duomenų saugos situacijai;
24.2. inventorizuojama VUSIS techninė ir programinė įranga;
24.3. peržiūrima VUSIS naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;
24.4. įvertinamas pasiruošimas VUSIS veiklai atkurti nenumatytose situacijose.

25. Atlikus VUSIS saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato Universiteto rektorius.

26. VUSIS elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra:

26.1. apsaugos sistema turi būti valdoma centralizuotai;
26.2. saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;
26.3. likutinė rizika turi būti sumažinta iki priimtino lygio;
26.4. būtina įdiegti prevencines informacijos saugos priemones.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. VUSIS administratorių ir naudotojų veiksmai, susiję su VUSIS duomenimis, reglamentuoti VUSIS nuostatuose, VUSIS tvarkymo taisyklėse, VUSIS naudotojų administravimo taisyklėse ir kituose VUSIS saugos politiką įgyvendinančiuose teisės aktuose.

28. Lokalaus tinklo, jungiančio tam tikro Universiteto padalinio kompiuterius ir tinklo serverius bei per Universiteto tarptinklinių ryšių mazgą turinčio išėjimą į Internetą, administratorius atsako už VUSIS naudotojų ir administratorių kompiuterinių darbo vietų (toliau – KDV) įrengimą ir naudojimą bei kompiuterių antivirusinių priemonių diegimą.

29. VUSIS naudotojų darbo vietose diegiamos aktyvios priemonės apsaugai nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programų, nepageidaujamų pašto žinučių platinimo ir panašiai). Šios priemonės turi būti atnaujinamos automatiškai ne rečiau kaip kartą per savaitę.

30. Visa VUSIS naudotojų kompiuteriuose įdiegta programinė įranga turi būti suderinta su lokalaus tinklo administratoriumi.

31. VUSIS naudotojai ir administratoriai kompiuterių programinę įrangą naudoja vadovaudamiesi Universiteto rektoriaus 2008-10-21 įsakymu Nr. R-351 patvirtinta Kompiuterių programų naudojimo tvarka Vilniaus universitete.

32. Visi prisijungimai prie VUSIS atliekami tik per šifruotą prieigą (SSL).

33. Ne iš Universiteto tinklo prieiga prie VUSIS komponentų, kuriuose galimas asmens duomenų tvarkymas, realizuojama naudojant virtualaus privataus tinko (VPN) paslaugą.

34. Nešiojamiems kompiuteriams, kurių vartotojams suteikta nuotolinės prieigos teisė prie komponentų, kuriuose galimas asmens duomenų tvarkymas, taikomos papildomos disko šifravimo ir kompiuterių rakinimo priemonės.

35. VUSIS administravimo prieiga prieinama tik iš suderintų vidinių IP adresų. Vartotojui skirtas IP adresų keitimas kontroliuojamas administracinėmis ir techninėmis priemonėmis.

36. VUSIS naudotojams prieigos prie VUSIS duomenų galimybė suteikiama tik per registravimosi ir slaptažodžių sistemą, prieigos sesijos laikas yra ribojamas. Prieigos suteikimo

tvarka ir sesijos trukmė darbuotojų kategorijoms reglamentuojama VUSIS naudotojų administravimo taisyklėse.

37. VUSIS vidinės tarnybos yra apsaugotos tinklo priemonėmis, išskiriant jas atskirame potinklyje.

38. VUSIS naudojamas kompiuterių tinklas yra dalinai filtruojamas nuo nepageidaujamo duomenų srauto.

39. VUSIS duomenų stotys saugomos programinėmis ugniasienėmis.

40. Universiteto kompiuterių tinklo saugumui užtikrinti veikia Universiteto CERT (Computer Emergency Response Team) – kompiuterinių incidentų tyrimo Universiteto tinkluose tarnyba.

41. Prieiga prie VUSIS administravimo funkcijų galima tik sistemos tvarkytojui suteikus teisę sistemos valdytojo teikimu, iš patvirtinto Universiteto vidinio tinklo IP sąrašo darbo vietų.

42. Automatiniu būdu duomenys perduodami arba gaunami tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas, naudojant saugų duomenų perdavimo protokolą.

43. Asmens duomenų perdavimas išorinėmis laikmenomis draudžiamas.

44. VUSIS veiklos tęstinumui ir funkcionalumui užtikrinti VUSIS duomenys periodiškai kopijuojami ir saugomi. VUSIS duomenų kopijų darymo periodiškumas, kopijų saugojimo priemonės, būdai ir vieta, kopijų atkūrimo tvarka, naikinimo tvarka reglamentuojama Informacinės sistemos duomenų bazių atsarginių kopijų darymo ir saugojimo tvarkoje, patvirtintoje 2008 m. spalio 29 d. įsakymu Nr. D–11.

45. Siekiant apsisaugoti nuo VUSIS tvarkomų duomenų praradimo ir užtikrinti efektyvią asmens duomenų apsaugą bei užkirsti kelią neteisėtam saugomų laikmenų naudojimui Universitete, nustatyta tokia informacinės sistemos duomenų bazių atsarginių kopijų darymo ir saugojimo tvarka:

45.1. Ribojamas darbuotojų, galinčių patekti į serverių sales, skaičius;

45.2. Vykdoma papildoma fizinės prieigos į duomenų centrą kontrolė (administracinėmis ir fizinės saugos priemonėmis);

45.3. Paskirti darbuotojai, atsakingi už kopijų darymą ir jų saugojimą;

45.4. Du kartus per savaitę daroma pilna VUSIS duomenų bazės kopija;

45.5. Inkrementinė kopija daroma du kartus į parą;

45.6. Kartą per parą kopijos perkopijuojamos į nutolusią magnetinių juostų biblioteką, esančią kitoje miesto vietoje (Universiteto centriniai rūmai, Universiteto g. 3, Vilnius).

45.7. Tris kartus per parą daromos bazės duomenų pakeitimų žurnalai (*archivelog*) kopijos;

45.8. Nutolusioje magnetinių juostų bibliotekoje saugomos keturių savaičių senumo VUSIS duomenų bazės kopijos;

45.9. Diskų masyve saugomos dviejų savaičių senumo VUSIS duomenų bazės kopijos;

45.10. Duomenų bazių atkūrimo bandymai atliekami kas šešis mėnesius;

45.11. Vėlesnių kaip dviejų savaičių duomenų bazių kopijos yra naikinamos naudojant sistemines priemones.

IV. REIKALAVIMAI PERSONALUI

46. VUSIS duomenims saugiai rinkti, apdoroti, sisteminti, kaupti, saugoti ir teikti duomenų gavėjams aktualią, kokybišką informaciją gali tik asmenys, susipažinę su VUSIS nuostatais, VUSIS saugos nuostatais, VUSIS saugos politiką įgyvendinančiais teisės aktais.

47. VUSIS duomenų saugos įgaliotinis privalo išmanyti pagrindinius informacijos saugos principus, išmanyti norminių teisės aktų reikalavimus, reglamentuojančius elektroninės informacijos saugą, turėti ir tobulinti kvalifikaciją elektroninės informacijos saugos srityje (kvalifikacijos tobulinimo kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL vartotojo sertifikatas ar pan.), turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties. VUSIS duomenų saugos įgaliotiniu negali būti skiriamas

asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, 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, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieneri metai.

48. VUSIS duomenų saugos įgaliotinis turi:

48.1. sugebėti vertinti VUSIS rizikos veiksnių tikėtumus ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

48.2. sugebėti vertinti VUSIS saugos politiką įgyvendinančius teisės aktus.

49. VUSIS padalinio administratorius turi:

49.1. būti susipažinęs su Universiteto studijų procesu, studijų procesą ir studijų organizavimo tvarką reglamentuojančiais Universiteto teisės aktais, studijų organizavimo tvarka;

49.2. sugebėti tvarkyti VUSIS duomenis VUSIS nuostatuose nustatyta tvarka;

49.3. būti supažindintas su VUSIS saugos politiką įgyvendinančiais teisės aktais.

50. VUSIS DB administratoriai turi:

50.1. išmanyti darbą su kompiuteriniais tinklais;

50.2. turėti sisteminių programinių priemonių Windows, Unix, Oracle administravimo patirties;

50.3. mokėti administruoti ir prižiūrėti registrų ir informacinių sistemų duomenų bazes.

51. VUSIS naudotojai turi:

51.1. turėti pagrindinius darbo su kompiuteriu įgūdžius;

51.2. mokėti tvarkyti VUSIS duomenis VUSIS nuostatuose nustatyta tvarka;

51.3. būti supažindinti su VUSIS saugos politiką įgyvendinančiais teisės aktais.

52. VUSIS naudotojams turi būti periodiškai (kas 1 metus arba papildomai, esant poreikiui) rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugumo problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams ir pan.).

53. Duomenų saugos mokymus ir priminimus apie saugumo problematiką vykdo VUSIS duomenų saugos įgaliotinis, VUSIS pagrindinis administratorius.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

54. VUSIS naudotojai saugiai dirbti su VUSIS duomenimis gali tik susipažinę su VUSIS saugos nuostatais, VUSIS saugos politiką įgyvendinančiais ir kitais teisės aktais, kuriais vadovaujamasi Universitete tvarkant elektroninę informaciją, ir pasirašytinai arba kitu būdu sutikę laikytis jų reikalavimų, jeigu užtikrinamas susipažinimo įrodomumas.

55. VUSIS naudotojai, prieš suteikiant jiems prieigą prie elektroninės informacijos, turi būti supažindinti su VUSIS saugos nuostatais bei šių nuostatų 3 punkte išvardintais VUSIS saugos politiką įgyvendinančiais teisės aktais, juose numatytais duomenų saugumo reikalavimais ir teisine atsakomybe už jų nesilaikymą.

56. VUSIS duomenų saugos įgaliotinis nedelsdamas supažindina pasirašytinai arba kitu būdu, jeigu užtikrinamas susipažinimo įrodomumas, VUSIS naudotojus su pakeistais VUSIS saugos nuostatais, VUSIS saugos politiką įgyvendinančiais teisės aktais.

57. Už VUSIS naudotojų saugaus darbo su VUSIS mokymo organizavimą yra atsakingas VUSIS duomenų saugos įgaliotinis.

VI. BAIGIAMOSIOS NUOSTATOS

58. Duomenys apie VUSIS naudotojų veiksmus su VUSIS duomenimis saugomi VUSIS tvarkytojo nustatyta tvarka ir terminais.

59. VUSIS naudotojai, pažeidę VUSIS saugos nuostatuose, VUSIS saugos politiką įgyvendinančiuose teisės aktuose nustatytas VUSIS duomenų saugaus tvarkymo nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.
