VILNIAUS UNIVERSITETO
REKTORIUS

ĮSAKYMAS
DĖL VILNIAUS UNIVERSITETO REKTORIAUS 2014 M. LAPKRIČIO 12 D. ĮSAKYMO NR. R-520 „DĖL AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2019 m. gruodžio d. Nr. R-
Vilnius

Vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 2 ir 3 dalimis, 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ 7 ir 8 punktais,

p a k e i č i u Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos duomenų saugos nuostatus, patvirtintus Vilniaus universiteto rektoriaus 2014 m. lapkričio 12 d. įsakymu Nr. R-520 „Dėl Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (su pakeitimais Vilniaus universiteto rektoriaus 2018 m. rugsėjo 25 d. įsakymu Nr. R-515) ir išdėstau juos nauja redakcija (pridedama).

Rektorius prof. Artūras Žukauskas

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie KAM
2019-08-30 raštu Nr. (4.2 E) 6K-564

Parengė:
Vilniaus universiteto Informacinių technologijų paslaugų centro
informacijos saugos vadovas
Viktoras Bulavas

PATVIRTINTA
Vilniaus universiteto rektoriaus
2014 m. lapkričio 17 d. įsakymu Nr. R-520
(Vilniaus universiteto rektoriaus
2019 m. gruodžio _ d. įsakymo Nr. R-___ redakcija)

AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Duomenų saugos nuostatai) reglamentuoja pagrindinius elektroninės informacijos saugos užtikrinimo ir valdymo principus, kuriais vadovaujantis turi būti įgyvendinama Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos (toliau – informacinė sistema) saugos politika, informacinės sistemos duomenų saugos procese dalyvaujančius subjektus, jų funkcijas, nustato organizacinius ir techninius duomenų saugos reikalavimus, informacinės sistemos naudotojų supažindinimo su informacinės sistemos saugos dokumentais principus.

2. Informacinės sistemos elektroninės informacijos saugumo užtikrinimo tikslai:

2.1. informacinės sistemos elektroninės informacijos vientisumo, prieinamumo ir konfidencialumo užtikrinimas;

2.2. saugaus duomenų tvarkymo automatiniu būdu sąlygų užtikrinimas.

3. Informacinės sistemos saugos užtikrinimo prioritetinės kryptys: saugus teisėtų, patikimų, apsaugotų nuo atsitiktinio panaudojimo ar neteisėto sunaikinimo, pakeitimo ir atskleidimo informacinės sistemos duomenų gavimas ir teikimas informacinės sistemos naudotojams, informacinės sistemos duomenų gavėjams, teisėtas, saugus ir kokybiškas informacinės sistemos duomenų tvarkymas, teisėtas ir saugus jų naudojimas bei veiklos tęstinumo užtikrinimas.

4. Informacinės sistemos valdytojas – Vilniaus universitetas, adresas - Universiteto g. 3, LT-01513 Vilnius.

5. Informacinės sistemos valdytojas:

5.1. turi visas Lietuvos Respublikos informacinių išteklių įstatyme ir Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos nuostatuose, patvirtintuose Vilniaus universiteto rektoriaus 2014 m. spalio 20 d. įsakymu Nr. R-473 „Dėl Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos nuostatų patvirtinimo“, (toliau – Informacinės sistemos nuostatai) nustatytas teises ir pareigas ir koordinuoja informacinės sistemos funkcionavimą;

5.2. turi teisę:

5.2.1. rengti ir priimti teisės aktus, susijusius su duomenų tvarkymu ir duomenų sauga;

5.2.2. spręsti informacinės sistemos plėtros klausimus;

5.2.3. perduoti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje numatytam paslaugos teikėjui informacinės sistemos techninės ir programinės įrangos priežiūrą ir (arba) informacijos tvarkymo funkcijų, išskyrus funkcijas, susijusias su sprendimų dėl informacijos teikimo ir skelbimo, ir su asmenų, tvarkančių informaciją, teisių ir pareigų nustatymo priėmimu, vykdymą;

5.2.4. dalį informacinės sistemos valdytojo funkcijų pavesti vykdyti savo struktūriniam padaliniui.

5.3. privalo:

5.3.1. koordinuoti pagrindinio informacinės sistemos tvarkytojo ir Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje numatyto paslaugų teikėjo darbą, teisės aktų nustatyta tvarka atlikti jų priežiūrą;

5.3.2. atlikti duomenų saugos reikalavimų laikymosi priežiūrą;

5.3.3. nagrinėti pagrindinio informacinės sistemos tvarkytojo pasiūlymus dėl informacinės sistemos veiklos tobulinimo ir priimti dėl jų sprendimus;

5.3.4. užtikrinti, kad informacinė sistema būtų tvarkoma vadovaujantis įstatymais, Informacinės sistemos nuostatais ir kitais teisės aktais;

5.4. vykdo kitas Informacinės sistemos nuostatuose, šiuose Duomenų saugos nuostatuose ir kituose informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

6. Žemiau įvardintas informacinės sistemos valdytojo funkcijas Vilniaus universitete atlieka Vilniaus universiteto Centrinės administracijos Studentų paslaugų ir karjeros skyrius, kuris:

6.1. organizuoja ir vadovauja informacinės sistemos veiklai;

6.2. koordinuoja informacinės sistemos duomenų saugos nuostatų, informacinės sistemos saugos politiką įgyvendinančių teisės aktų rengimą ir kontroliuoja jų įgyvendinimą;

6.3. koordinuoja informacinės sistemos funkcijų pokyčių planavimą, kuris apima pokyčių identifikavimą, suskirstymą į kategorijas ir prioritetų nustatymą;

6.4. koordinuoja sprendimų dėl informacinės sistemos techninių ir programinių priemonių įsigijimo, įdiegimo ir modernizavimo, priėmimą;

6.5. koordinuoja elektroninės informacijos tvarkymo teisėtumo priežiūrą ir užtikrinimą;

6.6. koordinuoja informacinės sistemos saugos politikos įgyvendinimą.

7. Pagrindinis informacinės sistemos tvarkytojas – Vilniaus universitetas, kurio toliau išvardintas funkcijas įgyvendina Vilniaus universiteto Informacinių technologijų paslaugų centras (adresas - Saulėtekio al. 9, II jungiamieji rūmai, LT-10222, Vilnius).

8. Pagrindinis informacinės sistemos tvarkytojas:

8.1. atsako už informacinei sistemai reikalingų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Duomenų saugos nuostatuose ir kituose informacinės sistemos saugos politiką įgyvendinančiuose teisės aktuose nustatyta tvarka.

8.2. skiria informacinės sistemos saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti Duomenų saugos nuostatų, kitų informacinės sistemos saugos politiką įgyvendinančių teisės aktų ir kitų Lietuvos Respublikos teisės aktų įgyvendinimą pagal kompetenciją;

8.3. užtikrina informacinės sistemos techninę priežiūrą, nepertraukiamą informacinės sistemos veikimą, informacinės sistemos duomenų ir dokumentų saugą;

8.4. teikia siūlymus informacinės sistemos valdytojui dėl informacinės sistemos eksploatavimui, priežiūrai ir plėtrai reikalingų techninių, programinių priemonių įsigijimo, organizuoja jų įdiegimą ir modernizavimą, pagal kompetenciją organizuoja informacinės sistemos techninės, programinės įrangos priežiūros ir tobulinimo darbus;

8.5. įgyvendina tinkamas organizacines ir technines priemones, skirtas informacinės sistemos duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo kito neteisėto veiksmo;

8.6. užtikrina, kad informacinės sistemos naudotojai laikytųsi reikalavimų, nustatytų Duomenų saugos nuostatuose ir kituose informacinės sistemos saugos politiką įgyvendinančiuose teisės aktuose;

8.7. užtikrina informacinės sistemos duomenų tvarkymo teisėtumą ir duomenų saugą;

8.8. skiria informacinės sistemos administratorius;

8.9. vykdo kitas Duomenų saugos nuostatuose, informacinės sistemos nuostatuose ir kituose informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

9. Informacinės sistemos tvarkytojai:

9.1. įgyvendina tinkamas organizacines ir technines priemones, skirtas informacinės sistemos duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo kito neteisėto veiksmo;

9.2. tvarko savo institucijos duomenis, kurie yra tvarkomi informacinėje sistemoje;

9.3. užtikrina, kad informacinės sistemos naudotojai laikytųsi reikalavimų, nustatytų Duomenų

saugos nuostatuose ir kituose informacinės sistemos saugos politiką įgyvendinančiuose teisės aktuose;

9.4. užtikrina informacinės sistemos duomenų tvarkymo teisėtumą ir duomenų saugą;

9.5. vykdo kitas Duomenų saugos nuostatais, informacinės sistemos nuostatais ir kitais Lietuvos Respublikos teisės aktais nustatytas funkcijas.

10. Informacinės sistemos saugos įgaliotinis:

10.1. atsako už informacinės sistemos duomenų saugos įgyvendinimą;

10.2. organizuoja kasmetį ir neeilinius informacinės sistemos rizikos vertinimus;

10.3. rengia informacinės sistemos rizikos įvertinimo ataskaitą;

10.4. koordinuoja incidentų, įvykusių informacinės sistemos duomenų saugos srityje, tyrimą;

10.5. periodiškai organizuoja informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais;

10.6. teikia informacinės sistemos taikomosios programinės įrangos administratoriams, informacinės sistemos naudotojų teisių ir sisteminiams administratoriams teisėtus nurodymus ir pavedimus, kuriuos jie privalo vykdyti;

10.7. teikia pasiūlymus informacinės sistemos pagrindiniam tvarkytojui dėl:

10.7.1. informacinės sistemos naudotojų teisių, taikomosios programinės įrangos administratorių ir sisteminių administratorių skyrimo;

10.7.2. saugos politiką įgyvendinančių teisės aktų ir kitų dokumentų priėmimo, keitimo ar panaikinimo;

10.7.3. informacinės sistemos saugos reikalavimų atitikties galiojantiems teisės aktams ir informacinės sistemos saugos reikalavimų atitikties vertinimo atlikimo ne rečiau kaip kartą per du metus;

10.8. vykdo kitas informacinės sistemos tvarkytojo pavestas ir teisės aktuose saugos įgaliotiniui priskirtas funkcijas.

11. Informacinės sistemos saugos įgaliotinis ir naudotojai negali atlikti administratoriaus funkcijų.

12. Informacinės sistemos taikomosios programinės įrangos administratorius:

12.1. užtikrina informacinės sistemos taikomosios programinės įrangos veikimą;

12.2. vykdo informacinės sistemos taikomosios programinės įrangos priežiūrą;

12.3. vykdo informacinės sistemos naudotojų ir jų prieigos teisių administravimą;

12.4. tvarko informacinės sistemos klasifikatorius;

12.5. konsultuoja vidinius informacinės sistemos naudotojus dėl informacinės sistemos naudojimo ir susijusiais klausimais;

12.6. vertina informacinės sistemos naudotojų pasirengimą dirbti su informacine sistema;

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

12.8. rengia ir tikrina informacinę sistemą sudarančių komponentų sąranką;

12.9. informuoja informacinės sistemos saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

12.10. vykdo informacinės sistemos saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

13. Informacinės sistemos sisteminis administratorius:

13.1. užtikrina informacinės sistemos sisteminės programinės įrangos ir duomenų bazių valdymo programinės įrangos veikimą;

13.2. atlieka informacinės sistemos sisteminės programinės įrangos ir duomenų bazių valdymo programinės įrangos priežiūrą;

13.3. atlieka atsarginių informacinės sistemos duomenų kopijų darymą;

13.4. atlieka visiškus ar dalinius duomenų atkūrimo bandymus iš atsarginių informacinėje sistemoje saugomų duomenų kopijų;

13.5. užtikrina informacinės sistemos sisteminės programinės įrangos saugą;

13.6. nustato informacinės sistemos pažeidžiamas vietas ir informuoja apie jas informacinės sistemos saugos įgaliotinį;

13.7. vykdo informacinės sistemos saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

14. informacinės sistemos naudotojų teisių administratorius:

14.1. tvarko ir administruoja savo institucijos valdomus informacinės sistemos duomenis;

14.2. vykdo savo institucijos informacinės sistemos naudotojų ir jų prieigos teisių administravimą;

14.3. vertina savo institucijos informacinės sistemos naudotojų pasirengimą dirbti su sistema;

14.4. atlieka savo institucijos naudotojams suteiktų informacinėje sistemoje teisių ir priskirtų funkcijų atitikties vertinimą;

14.5. konsultuoja savo institucijos naudotojus dėl informacinės sistemos veikimo ir kitais susijusiais klausimais;

14.6. reikalauja, kad institucijos naudotojai vykdytų informacinės sistemos duomenų saugos ir naudotojų administravimo taisyklių reikalavimus;

14.7. informuoja savo institucijos saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

14.8. vykdo pareigas ir reikalavimus, nurodytus kituose informacinės sistemos saugos politiką įgyvendinančiuose dokumentuose;

14.9. vykdo pagrindinio tvarkytojo saugos įgaliotinio ir pagrindinio tvarkytojo naudotojų administratoriaus nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

14.10. pagrindinio tvarkytojo naudotojų administratoriaus nurodymu vykdo kitas tiesiogiai su informacinės sistemos naudotojų teisių administravimu susijusias funkcijas.

15. Informacinės sistemos lokalaus tinklo ir darbo vietų administratorių funkcijos:

15.1. užtikrina savo institucijos lokalių tinklų veikimą;

15.2. prižiūri savo institucijos lokalius tinklus;

15.3. užtikrina informacinės sistemos naudotojų kompiuterinių darbo vietų saugą ir sklandų veikimą savo institucijoje;

15.4. prižiūri informacinės sistemos naudotojų kompiuterines darbo vietas savo institucijoje;

15.5. diegia, atnaujina antivirusines programas savo institucijos informacinės sistemos naudotojų darbo vietose;

15.6. vykdo pagrindinio tvarkytojo saugos įgaliotinio ir pagrindinio tvarkytojo naudotojų administratoriaus nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu;

15.7. vykdo kitas tiesiogiai su informacinės sistemos naudotojų lokalaus tinklo ir darbo vietų administravimu susijusias funkcijas.

16. Informacinės sistemos saugos nuostatai, kiti informacinės sistemos saugos politiką įgyvendinantys teisės aktai yra privalomi informacinės sistemos valdytojui, informacinės sistemos tvarkytojams, visiems informacinės sistemos administratoriams, informacinės sistemos saugos įgaliotiniams ir informacinės sistemos naudotojams.

17. Teisės aktai, kuriais vadovaujamasi tvarkant informacinės sistemos duomenis ir užtikrinant jų saugumą:

17.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

17.2. Lietuvos Respublikos elektroninių ryšių įstatymas;

17.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

17.4. Lietuvos Respublikos kibernetinio saugumo įstatymas;

17.5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

17.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio

saugumo subjektams, aprašas (toliau – kibernetinio saugumo reikalavimų aprašas), patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

17.7. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (toliau – Aprašas), Saugos dokumentų turinio gairių aprašas, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtinti Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

17.8. 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“;

17.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

17.10. Studijuojančiųjų asmens duomenų tvarkymo Vilniaus universitete taisyklės, patvirtintos Vilniaus universiteto senato komisijos 2013 m. birželio 20 d. nutarimu Nr. SK-2013-8-7;

17.11. Vilniaus universiteto darbo tvarkos taisyklės, patvirtintos Vilniaus universiteto rektoriaus 2015 m. balandžio 20 d. įsakymu Nr. R-146;

17.12. Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklės, patvirtintos Lietuvos Respublikos švietimo ir mokslo ministro 2011 m. liepos 18 d. įsakymu Nr. V-1348 „Dėl Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET paslaugų teikimo tvarkos aprašo ir Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklių patvirtinimo“;

17.13. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai).

17.14. Informacinės sistemos nuostatai;

17.15. Duomenų saugos nuostatai;

17.16. Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

17.17. Informacinės sistemos veiklos tęstinumo valdymo planas;

17.18. Informacinės sistemos naudotojų administravimo taisyklės.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ 9.1, 9.3 ir 12.3 papunkčių nuostatomis, informacinėje sistemoje tvarkoma elektroninė informacija pagal jos svarbą laikoma vidutinės svarbos elektronine informacija, o informacinė sistema priskiriama trečios kategorijos informacinėms sistemoms.

19. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja informacinės sistemos rizikos įvertinimą. Pasikeitus informacinės sistemos funkcinei sandarai, atsiradus naujiems rizikos veiksniams, informacinės sistemos tvarkytojo vadovo pavedimu informacinės sistemos saugos įgaliotinis organizuoja neeilinį informacinės sistemos rizikos įvertinimą.

20. 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 informacinės sistemos duomenims, programinei, techninei įrangai yra:

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

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

20.3. 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.

21. Atlikus rizikos įvertinimą, esant poreikiui, informacinės sistemos saugos įgaliotinis rengia ir teikia informacinės sistemos tvarkytojo funkcijas atliekančio padalinio vadovui tvirtinti rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Pagrindiniai informacinės sistemos duomenų saugos priemonių parinkimo principai yra šie:

22.1. įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;

22.2. taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina;

22.3. naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;

22.4. likutinė rizika turi būti sumažinama iki saugos politiką įgyvendinančiuose dokumentuose numatytų reikalavimų atitikties lygio;

22.5. duomenų saugos priemonės diegimo kaina turi būti adekvati saugomų duomenų vertei;

22.6. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės duomenų saugos priemonės;

22.7. šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

23. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

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

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

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

27. informacinės sistemos saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per du metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba Universitete įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių. Keičiami saugos dokumentai derinami su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos Aprašo nustatyta tvarka. Keičiami saugos dokumentai gali būti nederinami tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

28. Patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

29. Informacinės sistemos naudotojų darbo vietose draudžiama naudoti programinę įrangą, galinčią kelti grėsmę informacinės sistemos duomenų saugumui.

30. Informacinės sistemos tarnybinėse stotyse, administratorių ir naudotojų kompiuterinėse darbo vietose turi būti įdiegta legali ir saugi programinė įranga (operacinė sistema su naujausiais pataisymais).

31. Informacinės sistemos naudotojų sąsaja pasiekiama per internetinę naršyklę. Duomenų perduodamų tarp tarnybinės stoties ir naudotojo darbo vietų saugumas užtikrinamas naudojant saugų HTTPS protokolą.

32. Kompiuterinis tinklas, prie kurio prijungtos informacinės sistemos tarnybinės stotys, nuo viešojo interneto yra atskirtas užkarda (angl. firewall), DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga.

33. Priemonės ir metodai, kurie taikomi užtikrinant prieigą prie informacinės sistemos, nurodant leistiną šios prieigos laiką ir būdą, nustatomi informacinės sistemos naudotojų administravimo taisyklėse.

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

34.1. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

34.2. naudojama tik legali programinė įranga;

34.3. programinė įranga yra nuolatos atnaujinama laikantis gamintojo reikalavimų;

34.4. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik informacinės sistemos administratoriai.

35. Informacinės sistemos veiklos tęstinumui užtikrinti informacinės sistemos duomenys yra periodiškai kiekvieną darbo dieną kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad kilus elektroninės informacijos saugos incidentui informacinės sistemos veiklą iš atsarginių kopijų būtų galima atstatyti per 16 valandų. Rezervinių kopijų laikmenos saugomos fiziškai nutolusiose patalpose.

36. Visuose informacinės sistemos vidinių naudotojų darbo vietų kompiuteriuose ir tarnybinėse stotyse turi būti įdiegiama apsaugos nuo virusų ir kitos nepageidaujamos programinės įrangos sistema, kuri turi tikrinti ar nėra atnaujinimų bent vieną kartą per parą. Nustačius, jog

apsaugos nuo virusų ir kitos nepageidaujamos programinės įrangos sistemos atnaujinimai yra prieinami – jie turi būti ištestuojami ir įdiegiami.

37. Informacinės sistemos vidiniai naudotojai, vadovaudamiesi saugos politiką įgyvendinančiais teisės aktais, nuolat rūpinasi informacinės sistemos sauga, o pastebėję saugos pažeidimų, neveikiančias duomenų saugos užtikrinimo priemones, nusikalstamos veikos požymių, privalo nedelsdami apie tai pranešti informacinės sistemos taikomosios programinės įrangos administratoriui arba lokalaus tinklo arba darbo vietos administratoriui.

38. Informacinės sistemos vidinių naudotojų veiksmus esant nenumatytai situacijai reglamentuoja informacinės sistemos veiklos tęstinumo valdymo planas, kurį pagrindiniam informacinės sistemos tvarkytojui teikia informacinės sistemos saugos įgaliotinis.

39. Prieigai prie informacinės sistemos naudojami kompiuteriai gali būti naudojami ir kitoms informacinės sistemos naudotojo ar informacinės sistemos administratoriaus funkcijoms atlikti.

40. informacinės sistemos administravimo funkcijoms naudojamus kompiuterius leidžiama naudoti tik informacinės sistemos tvarkytojų įstaigos patalpose. Mobilių įrenginių naudojimas administravimo reikmėms neleidžiamas.

41. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal paslaugų teikimo sutartyse nustatytas specifikacijas ir sąlygas, įsipareigojusiems saugoti asmens duomenų konfidencialumo reikalavimų naudotojams.

42. Naudotojų prisijungimo prie informacinės sistemos saugomų asmens duomenų įrašai saugomi ne trumpiau kaip 1 metus, ir naikinami bendra tvarka. Fiksuojami šie prisijungimų prie asmens duomenų įrašai: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas), panaudoto įrenginio informacija (IP adresas).

43. Informacinės sistemos naudotojų prisijungimo duomenys saugomi ne trumpiau, nei 90 kalendorinių dienų ir ne ilgiau, kaip 1 metus nuo informacinės sistemos naudotojo paskyros uždarymo.

44. Informacinės sistemos stebėsenai reikalingi duomenys saugomi visą stebėsenos laikotarpį (5 metus nuo pirmo stebėsenos duomenų pateikimo).

45. Pasibaigus šiuose Duomenų saugos nuostatuose nurodytiems duomenų saugojimo terminams, informacinės sistemos duomenys sunaikinami Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti archyvams.

46. Informacinės sistemos duomenų kopijų darymo periodiškumas, kopijų saugojimo priemonės, būdai ir vieta, kopijų naikinimo tvarka reglamentuojama informacinės sistemos rezervinio kopijavimo ir atstatymo instrukcijoje, kurią tvirtina pagrindinis informacinės sistemos tvarkytojas.

47. informacinės sistemos atstatymo iš atsarginių kopijų procedūros reglamentuojamos informacinės sistemos duomenų atstatymo iš atsarginių kopijų tvarkoje, kurią tvirtina pagrindinis informacinės sistemos tvarkytojas.

48. Nustatomi šie minimalūs organizaciniai – techniniai informacinės sistemos duomenų atsarginių kopijų darymo, saugojimo ir atstatymo saugos reikalavimai:

48.1. Priimtinas informacinės sistemos valdytojui prarastų duomenų kiekis – 4 valandos;

48.2. paskirti darbuotojai, atsakingi už informacinės sistemos kopijų darymą, saugojimą ir atstatymą;

48.3. kiekvienas informacinės sistemos elektroninės informacijos kopijų darymo ir atstatymo faktas turi būti užregistruotas;

48.4. atsarginės kopijos saugomos kitose patalpose, nei darbinės duomenų kopijos;

48.5. informacinės sistemos duomenų atkūrimo bandymai atliekami ne rečiau, kaip kartą į metus;

48.6. informacinės sistemos laikmenos saugomos taip, kad kilus elektroninės informacijos saugos incidentui informacinės sistemos veiklą rezerviniame duomenų centre galima būtų atstatyti per 24 valandas;

48.7. informacinės sistemos duomenų atsarginių kopijų darymo, saugojimo ir atstatymo tvarkos ir instrukcijos turi būti peržiūrimos ne rečiau, kaip kartą į metus.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

49. Informacinės sistemos saugos įgaliotinis ir administratoriai turi išmanyti informacijos saugos užtikrinimo principus (informacijos, konfidencialumo, vientisumo, pasiekiamumo apsaugos principus; organizacines apsaugos priemones, technines apsaugos priemones, apsaugos informacinių priemonių visumą), ir savo darbe vadovautis Aprašu ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais.

50. Saugos įgaliotiniu ir administratoriais 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 vieni metai.

51. Informacinės sistemos saugos įgaliotinis ir informacinės sistemos administratoriai turi išmanyti darbą su kompiuteriniais tinklais, mokėti užtikrinti jų saugumą, žinoti Duomenų saugos nuostatus, Informacinės sistemos nuostatus, saugos politiką įgyvendinančius teisės aktus;

52. Informacinės sistemos sisteminis administratorius turi išmanyti duomenų bazių administravimą, priežiūrą, žinoti Duomenų saugos nuostatus, Informacinės sistemos nuostatus, saugos politiką įgyvendinančius teisės aktus;

53. Informacinės sistemos taikomosios programinės įrangos administratorius turi išmanyti taikomosios programinės įrangos administravimą, priežiūrą, žinoti Duomenų saugos nuostatus, Informacinės sistemos nuostatus, saugos politiką įgyvendinančius teisės aktus;

54. Informacinės sistemos naudotojai turi turėti pagrindinius darbo su kompiuteriu įgūdžius ir turi būti susipažinę su Duomenų saugos nuostatais, saugos politiką įgyvendinančiais teisės aktais;

55. Informacinės sistemos saugos mokymų planavimo, organizavimo ir vykdymo tvarka:

55.1. informacinės sistemos vidiniai naudotojai ir administratoriai periodiškai (ne rečiau, kaip kartą į metus) įvairiomis priemonėmis informuojami apie saugumo problematiką, (pvz., priminimai elektroniniu paštu, atmintinės ir pan.).

55.2. Pirminį informacinės sistemos administratorių duomenų saugos instruktažą, prieš suteikiant prieigos teises, atlieka pagrindinio informacinės sistemos tvarkytojo naudotojų teisių administratorius;

55.3. Pakartotinis informacinės sistemos administratorių supažindinimas (instruktažas) su duomenų saugos reikalavimais vykdomas atnaujinus saugos dokumentus, išskyrus tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika;

55.4. mokymus turi vykdyti saugos įgaliotinis ar kitas darbuotojas, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymų paslaugų teikėjas.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS POLITIKĄ ĮGYVENDINANČIAIS TEISĖS AKTAIS PRINCIPAI

56. Informacinės sistemos naudotojai, prieš suteikiant jiems prieigą prie elektroninės informacijos, turi būti supažindinti su Duomenų saugos nuostatais bei informacinės sistemos saugos politiką įgyvendinančiais ir kitais saugų darbą su informacija reglamentuojančiais teisės aktais, juose numatytais duomenų saugumo reikalavimais ir teisine atsakomybe už jų nesilaikymą.

57. Pakartotinai informacinės sistemos naudotojai su Duomenų saugos nuostatais bei informacinės sistemos saugos politiką įgyvendinančiais ir kitais saugų darbą su informacija reglamentuojančiais teisės aktais supažindinami tada, kai šie iš esmės pasikeičia. Informacija apie pasikeitimus saugos politiką įgyvendinančiuose teisės aktuose siunčiama elektroniniu būdu.

58. Naudotojų ir administratorių supažindinimas vykdomas pasirašytinai arba elektroniniu būdu, užtikrinant susipažinimo įrodomumą.

59. Asmenys, pažeidę informacinės sistemos duomenų saugos nuostatų ir saugos politiką įgyvendinančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymuose ir kituose teisės aktuose nustatyta tvarka.

60. Informacinės sistemos saugos nuostatai ir informacinės sistemos saugos politiką įgyvendinantys teisės aktai skelbiami informacinės sistemos tinklalapyje.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Vilniaus universitetas 211950810, Universiteto g. 3, 01513 Vilnius
Dokumento pavadinimas (antraštė)	DĖL VILNIAUS UNIVERSITETO REKTORIAUS 2014 M. LAPKRIČIO 12 D. ĮSAKYMO NR. R-520 „DĖL AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO
Dokumento registracijos data ir numeris	2019-12-09 Nr. R-622
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Vizavimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Arūnas Stašionis, Direktorius, Informacinių technologijų paslaugų centras
Sertifikatas išduotas	ARŪNAS,STAŠIONIS LT
Parašo sukūrimo data ir laikas	2019-12-09 12:24:22 (GMT+02:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2019-01-23 12:56:45 – 2024-01-22 23:59:59
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Artūras Žukauskas, Rektorius, Centrinė administracija
Sertifikatas išduotas	ARTŪRAS,ŽUKAUSKAS LT
Parašo sukūrimo data ir laikas	2019-12-09 16:05:41 (GMT+02:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2019-12-09 16:06:00 (GMT+02:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2019-08-12 11:16:51 – 2024-08-10 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Vilniaus universitetas, į.k. 211950810 LT", sertifikatas galioja nuo 2018-12-27 14:18:54 iki 2021-12-26 14:18:54
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.13
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2019-12-09 16:13:30)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2019-12-09 16:13:30 Dokumentų valdymo sistema Avilys