1601356

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

2018 m. rugsėjo 25 d. Nr. R- 515
Vilnius

Vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 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“ 8 punktu bei Vilniaus universiteto Statuto 43 straipsnio 1 dalies 19 punktu,

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“ ir išdėstau juos nauja redakcija (pridedama).

Rektorius prof. Artūras Žukauskas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Lietuvos Respublikos krašto apsaugos ministerijos
2018 m. rugsėjo 13 d. raštu Nr. (4.2) 6K-573

Parengė:
Informacinių technologijų taikymo centro informacijos saugos vadovas
Viktoras Bulavas

PATVIRTINTA
Vilniaus universiteto rektoriaus
2014 m. lapkričio 17 d. įsakymu Nr. R-520
(Vilniaus universiteto rektoriaus
2018 m. rugsėjo 25 d. įsakymo Nr. R- 515
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 – KVIS) saugos politika (toliau – KVIS saugos politika), KVIS duomenų saugos procese dalyvaujančius subjektus, jų funkcijas, nustato organizacinius ir techninius duomenų saugos reikalavimus, KVIS naudotojų supažindinimo su KVIS saugos dokumentais principus.

2. KVIS elektroninės informacijos saugumo užtikrinimo tikslai:

2.1. KVIS elektroninės informacijos vientisumo, prieinamumo ir konfidencialumo užtikrinimas;

2.2. saugaus duomenų tvarkymo automatiniu būdu sąlygų užtikrinimas.

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

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

5. KVIS valdytojas:

5.1. vadovauja pagrindiniam tvarkytojui ir koordinuoja KVIS funkcionavimą;

5.2. turi teisę:

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

5.2.2. spręsti KVIS plėtros klausimus;

5.2.3. perduoti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje numatytam paslaugos teikėjui KVIS 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 KVIS valdytojo funkcijų pavesti vykdyti savo struktūriniam padaliniui.

5.3. privalo:

5.3.1. koordinuoti pagrindinio KVIS 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 KVIS tvarkytojo pasiūlymus dėl KVIS veiklos tobulinimo ir priimti dėl jų sprendimus;

5.3.4. užtikrinti, kad KVIS būtų tvarkoma vadovaujantis įstatymais, KVIS nuostatais ir kitais teisės aktais;

5.4. vykdo kitas KVIS nuostatuose, šiuose duomenų saugos nuostatuose ir kituose KVIS duomenų tvarkymo teisėtumą ir saugos valdymą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

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

6.1. organizuoja ir vadovauja KVIS veiklai;

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

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

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

6.5. koordinuoja elektroninės informacijos tvarkymo teisėtumo priežiūrą ir užtikrinimą;

6.6. koordinuoja KVIS saugos politikos įgyvendinimą.

7. Pagrindinis KVIS tvarkytojas – Vilniaus universiteto Informacinių technologijų paslaugų centras (adresas - Saulėtekio al. 9, II jungiamieji rūmai, LT-10222, Vilnius).

8. Pagrindinis KVIS tvarkytojas:

8.1. atsako už KVIS reikalingų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi KVIS duomenų saugos nuostatuose ir kituose KVIS saugos politiką įgyvendinančiuose teisės aktuose nustatyta tvarka.

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

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

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

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

8.6. užtikrina, kad KVIS naudotojai laikytųsi reikalavimų, nustatytų KVIS duomenų saugos nuostatuose ir kituose KVIS saugos politiką įgyvendinančiuose teisės aktuose;

8.7. užtikrina KVIS duomenų tvarkymo teisėtumą ir duomenų saugą;

8.8. skiria KVIS administratorius;

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

9. KVIS tvarkytojai privalo:

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

9.2. tvarkyti savo institucijos duomenis, kurie yra tvarkomi KVIS;

9.3. užtikrinti, kad KVIS naudotojai laikytųsi reikalavimų, nustatytų KVIS duomenų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose;

9.4. užtikrinti KVIS duomenų tvarkymo teisėtumą ir duomenų saugą;

9.5. vykdyti kitas KVIS duomenų saugos nuostatais, KVIS nuostatais ir kitais Lietuvos Respublikos teisės aktais nustatytas funkcijas.

10. KVIS saugos įgaliotinis:

10.1. atsako už KVIS duomenų saugos įgyvendinimą;

10.2. organizuoja kasmetį ir neeilinius KVIS rizikos vertinimus;

10.3. rengia KVIS rizikos įvertinimo ataskaitą;

10.4. koordinuoja incidentų, įvykusių KVIS duomenų saugos srityje, tyrimą;

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

10.6. teikia KVIS taikomosios programinės įrangos administratoriams, KVIS sisteminiams administratoriams ir KVIS techninės įrangos ir tinklų administratoriams teisėtus nurodymus ir pavedimus, kuriuos jie privalo vykdyti;

10.7. teikia pasiūlymus KVIS pagrindiniam tvarkytojui dėl:

10.7.1. KVIS taikomosios programinės įrangos administratorių, KVIS sisteminių administratorių ir KVIS techninės įrangos ir tinklų administratorių skyrimo;

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

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

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

11. KVIS Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

12. KVIS taikomosios programinės įrangos administratorius:

12.1. užtikrina KVIS taikomosios programinės įrangos veikimą;

12.2. vykdo KVIS taikomosios programinės įrangos priežiūrą;

12.3. vykdo KVIS naudotojų ir jų prieigos teisių administravimą;

12.4. vertina KVIS naudotojų pasirengimą dirbti su KVIS;

12.5. atlieka KVIS naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

12.6. rengia ir tikrina KVIS sudarančių komponentų sąranką;

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

12.8. vykdo KVIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

13. KVIS sisteminis administratorius:

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

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

13.3. atlieka atsarginių KVIS duomenų kopijų darymą;

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

13.5. užtikrina KVIS sisteminės programinės įrangos saugą;

13.6. nustato KVIS pažeidžiamas vietas ir informuoja apie juos KVIS saugos įgaliotinį;

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

14. KVIS techninės įrangos ir kompiuterių tinklų administratorius:

14.1. projektuoja, diegia ir plėtoja KVIS techninę įrangą ir kompiuterių tinklus;

14.2. užtikrina KVIS techninės įrangos ir kompiuterinių tinklų veikimą;

14.3. atlieka KVIS techninės įrangos ir kompiuterinių tinklų priežiūrą;

14.4. užtikrina KVIS kompiuterinio tinklo saugumą;

14.5. organizuoja darbą kompiuterių tinkle;

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

14.7. vykdo KVIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

15. KVIS saugos nuostatai, kiti KVIS saugos politiką įgyvendinantys teisės aktai yra privalomi KVIS valdytojui, KVIS tvarkytojams, visiems KVIS administratoriams, KVIS saugos įgaliotiniui ir KVIS naudotojams.

16. Teisės aktai, kuriais vadovaujamasi tvarkant KVIS duomenis ir užtikrinant jų saugumą:

16.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

16.2. Lietuvos Respublikos elektroninių ryšių įstatymas;

16.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

16.4. Lietuvos Respublikos kibernetinio saugumo įstatymas;

16.5. 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;

16.6. 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“;

16.7. 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 Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

16.8. 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“;

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

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

16.11. KVIS nuostatai;

16.12. KVIS duomenų saugos nuostatai;

16.13. KVIS saugaus elektroninės informacijos tvarkymo taisyklės;

16.14. KVIS veiklos tęstinumo valdymo planas;

16.15. KVIS naudotojų administravimo taisyklės.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. 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, KVIS tvarkoma elektroninė informacija pagal jos svarbą laikoma

vidutinės svarbos elektronine informacija, o KVIS priskiriama trečios kategorijos informacinėms sistemoms.

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

19. 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 KVIS duomenims, programinei, techninei įrangai yra:

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

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

19.3. 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.

20. Atlikus rizikos įvertinimą, esant poreikiui, KVIS saugos įgaliotinis rengia ir teikia KVIS valdytojo vadovui tvirtinti rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

21. Pagrindiniai KVIS duomenų saugos priemonių parinkimo principai yra šie:

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

21.2. 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;

21.3. 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;

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

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

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

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

22. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas KVIS 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.

23. Siekiant užtikrinti šiuose duomenų saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, KVIS 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 KVIS saugos atitikties vertinimą, kurio metu:

23.1. įvertinama šių nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų ir realios

informacijos saugos atitiktis;

23.2. patikrinama (įvertinama) KVIS naudotojams suteiktų teisių atitiktis vykdomoms funkcijoms;

23.3. įvertinamas pasirengimas užtikrinti KVIS veiklos tęstinumą įvykus saugos incidentui (nenumatytai situacijai).

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

25. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas KVIS 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.

26. KVIS 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.

27. Patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas KVIS 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
KVIS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. KVIS naudotojų darbo vietose draudžiama naudoti programinę įrangą, galinčią kelti grėsmę KVIS duomenų saugumui.

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

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

31. Kompiuterinis tinklas, prie kurio prijungtos KVIS tarnybinės stotys, nuo viešojo interneto yra atskirtas užkarda (angl. firewall).

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

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

34. Visuose KVIS 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 įdiegiami.

35. KVIS vidiniai naudotojai, vadovaudamiesi saugos politiką įgyvendinančiais teisės aktais, nuolat rūpinasi KVIS sauga, o pastebėję saugos pažeidimų, neveikiančias duomenų

saugos užtikrinimo priemones, nusikalstamos veikos požymių, privalo nedelsdami apie tai pranešti KVIS taikomosios programinės įrangos administratoriui arba KVIS techninės įrangos ir kompiuterių tinklų administratoriui.

36. KVIS vidinių naudotojų veiksmus esant nenumatytai situacijai reglamentuoja KVIS veiklos tęstinumo valdymo planas, kurį pagrindiniam KVIS tvarkytojui teikia KVIS saugos įgaliotinis.

37. Prieigai prie KVIS naudojami kompiuteriai gali būti naudojami ir kitoms KVIS naudotojo ir KVIS administratoriaus funkcijoms atlikti.

38. KVIS administravimo funkcijoms naudojamus kompiuterius leidžiama naudoti tik KVIS tvarkytojų įstaigos patalpose. Mobilių įrenginių naudojimas administravimo reikmėms neleidžiamas.

39. Duomenys teikiami ir (ar) gaunami automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

40. Naudotojų prisijungimo prie KVIS 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).

41. KVIS naudotojų prisijungimo duomenys saugomi ne trumpiau, nei 90 kalendorinių dienų ir ne ilgiau, kaip 1 metus nuo KVIS naudotojo paskyros uždarymo.

42. KVIS stebėsenai reikalingi duomenys saugomi visą stebėsenos laikotarpį (5 metus nuo pirmo stebėsenos duomenų pateikimo).

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

44. KVIS duomenų kopijų darymo periodiškumas, kopijų saugojimo priemonės, būdai ir vieta, kopijų naikinimo tvarka reglamentuojama KVIS rezervinio kopijavimo ir atstatymo instrukcijoje, patvirtintoje Informacinių technologijų taikymo centro direktoriaus 2015 m. balandžio 24 d. įsakymu Nr. DI-6-(5201.DĮ).

45. KVIS atstatymo iš atsarginių kopijų procedūros reglamentuojamos KVIS duomenų atstatymo iš atsarginių kopijų tvarkoje, patvirtintoje Informacinių technologijų taikymo centro direktoriaus 2015 m. balandžio 24 d. įsakymu Nr. DI-6-(5201.DĮ).

46. Nustatomi šie minimalūs organizaciniai – techniniai KVIS duomenų atsarginių kopijų darymo, saugojimo ir atstatymo saugos reikalavimai:

46.1. Priimtinas KVIS valdytojui prarastų duomenų kiekis – 4 valandos;

46.2. paskirti darbuotojai, atsakingi už KVIS kopijų darymą, saugojimą ir atstatymą;

46.3. kiekvienas KVIS elektroninės informacijos kopijų darymo ir atstatymo faktas turi būti užregistruotas;

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

46.5. KVIS duomenų atkūrimo bandymai atliekami ne rečiau, kaip kartą į metus;

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

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

IV SKYRIUS
REIKALAVIMAI PERSONALUI

47. KVIS saugos įgaliotinis 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.

48. Remiantis Aprašo 20 punkto nuostatomis, 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 vieni metai.

49. KVIS techninės įrangos ir kompiuterių tinklų administratorius turi išmanyti darbą su kompiuteriniais tinklais, mokėti užtikrinti jų saugumą, žinoti KVIS duomenų saugos nuostatus, KVIS nuostatus, saugos politiką įgyvendinančius teisės aktus;

50. KVIS sisteminis administratorius turi išmanyti duomenų bazių administravimą, priežiūrą, žinoti KVIS duomenų saugos nuostatus, KVIS nuostatus, saugos politiką įgyvendinančius teisės aktus;

51. KVIS taikomosios programinės įrangos administratorius turi išmanyti taikomosios programinės įrangos administravimą, priežiūrą, žinoti KVIS duomenų saugos nuostatus, KVIS nuostatus, saugos politiką įgyvendinančius teisės aktus;

52. KVIS naudotojai turi turėti pagrindinius darbo su kompiuteriu įgūdžius ir turi būti susipažinę su KVIS duomenų saugos nuostatais, saugos politiką įgyvendinančiais teisės aktais;

53. KVIS saugos mokymų planavimo, organizavimo ir vykdymo tvarka:

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

53.2. Pirminį KVIS administratorių duomenų saugos instruktažą, prieš suteikiant prieigos teises, atlieka pagrindinio KVIS tvarkytojo naudotojų teisių administratorius;

53.3. Pakartotinis KVIS administratorių supažindinimas (instruktažas) su duomenų saugos reikalavimais vykdomas atnaujinus saugos dokumentus;

53.4. 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

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

55. Pakartotinai KVIS naudotojai su KVIS saugos nuostatais bei KVIS 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.

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

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

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

58. KVIS saugos nuostatai ir KVIS saugos politiką įgyvendinantys teisės aktai skelbiami KVIS tinklalapyje.

_____