VILNIAUS UNIVERSITETO
REKTORIUS

ĮSAKYMAS
DĖL VILNIAUS UNIVERSITETO REKTORIAUS 2015 M. GEGUŽĖS 4 D. ĮSAKYMO NR. R-169 „DĖL AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ 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 Vilniaus universiteto rektoriaus 2015 m. gegužės 4 d. įsakymu Nr. R-169 „Dėl Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“:

1. Pakeičiu nurodytuoju įsakymu patvirtintas Saugaus elektroninės informacijos tvarkymo taisykles ir išdėstau jas nauja redakcija (pridedama);
2. Pakeičiu nurodytuoju įsakymu patvirtintą Veiklos tęstinumo valdymo planą ir išdėstau jį nauja redakcija (pridedama);
3. Pakeičiu nurodytuoju įsakymu patvirtintas Naudotojų administravimo taisykles ir išdėstau jas 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
2015 m. gegužės 4 d. įsakymu Nr. R-169
(Vilniaus universiteto rektoriaus
2019 m. gruodžio d. įsakymo Nr. R-
redakcija)

AUKŠTŲJŲ MOKYKLŲ STUDENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau –Taisyklės) nustato pagrindinio Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos (toliau – KVIS) tvarkytojo, jo paskirtų KVIS administratorių, KVIS saugos įgaliotinio, kitų KVIS tvarkytojų ir KVIS naudotojų veiksmus, užtikrinančius saugų KVIS techninės ir programinės įrangos funkcionavimą, KVIS duomenų tvarkymą ir teikimą KVIS duomenų teikėjams.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716„Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu, Nr. 1V-832 „Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2014 m. spalio 20 d. įsakymu R-473 „Dėl Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos nuostatų patvirtinimo“ (toliau – Informacinės sistemos nuostatai), Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos duomenų saugos nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2014 m. lapkričio 17 d. įsakymu R-520 „Aukštųjų mokyklų studentų karjeros valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Duomenų saugos nuostatai), taip pat kitais teisės aktais ir standartais, reglamentuojančiais duomenų tvarkymo teisėtumą, tvarkytojų veiklą ir duomenų saugos valdymą.

3. Taisyklės taikomos KVIS valdytojui ir KVIS tvarkytojams, visiems KVIS naudotojams, KVIS duomenų valdymo ir saugos įgaliotiniui ir administratoriams.

4. Visi KVIS naudotojai ir administratoriai, KVIS duomenų valdymo ir KVIS saugos įgaliotinis susipažįsta ir sutinka su šiomis Taisyklėmis pasirašytinai arba elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

5. Taisyklėse naudojamos sąvokos:

5.1. organizacinis KVIS naudotojas – informacinės sistemos naudotojas, darbo santykiais susijęs su organizacija, pasirašiusia su KVIS valdytoju sistemos naudojimo ir duomenų gavimo sutartį, nuostatų 18.1.4 punkte numatytiems tikslams įgyvendinti;

5.2. Taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Informacinės sistemos nuostatuose, Duomenų saugos

nuostatuose ir kituose teisės aktuose bei saugų duomenų tvarkymą reglamentuojančiuose standartuose.

6. KVIS informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių) sąrašas pateikiamas Informacinės sistemos nuostatų 15 punkte.

7. KVIS tvarkoma informacija yra skirstoma į šias grupes:

7.1. administratorių tvarkoma informacija;

7.2. naudotojų tvarkoma informacija.

8. Taikomosios programinės įrangos administratorius atsakingas už šios informacijos tvarkymą:

8.1. klasifikatoriai;

8.2. naudotojų duomenys;

8.3. naudotojų rolės;

8.4. naudotojų teisės;

8.5. naudotojų unikalūs identifikatoriai;

8.6. aukštųjų mokyklų karjeros centrų ir organizacijų paskyros;

8.7. bendras sistemos turinys (testai ir stebėsenos klausimynai, bendras portalo puslapių turinys, forumai, pagalbos centro turinys).

9. Sisteminis administratorius atsakingas už šios informacijos tvarkymą:

9.1. paslaugų iniciavimo ir teikimo duomenys;

9.2. paslaugų teikimą aprašantys duomenys;

9.3. paslaugų teikimo stebėsenos duomenys:

9.3.1. duomenų užklausimo laikas;

9.3.2. duomenų perdavimo laikas;

9.3.3. paslaugų suteikimo laikas;

9.3.4. kiti techniniai duomenys paslaugų teikimo stebėsenai atlikti.

10. KVIS naudotojai atsakingi už Informacinės sistemos nuostatų 15 punkte aprašytos informacijos tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

11. Saugiam KVIS elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės, kurių pagalba:

11.1. per metus informacinės sistemos prieinamumas turi būti užtikrintas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

11.2. informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei (trečios kategorijos informacinės sistemos) – 16 val.

12. Kompiuterinės įrangos saugos priemonės:

12.1. prieigos prie KVIS tarnybinių stočių (serverių) kontrolė užtikrinama suteikiant prieigos teises tik autorizuotiems asmenims, kuriems pagal atliekamas funkcijas prieiga prie KVIS tarnybinių stočių turi būti suteikta, o jų veiksmai, užtikrinantys KVIS duomenų apsaugą, aprašyti KVIS duomenų saugos nuostatuose;

12.2. KVIS naudotojų ir administratorių įgaliojimai, teisės ir pareigos nustatomos KVIS naudotojų administravimo taisyklėse;

12.3. svarbiausi kompiuterinės įrangos komponentai sujungiami klasteriniu režimu (angl. computer cluster), t.y. dubliuojant svarbiausią kompiuterinę įrangą, šios kompiuterinės įrangos techninės būklės nuolatinė stebėsena;

12.4. kompiuterinės įrangos gedimų registravimas vykdomas kompiuterinės įrangos gedimų žurnale;

12.5. KVIS administratorių ir vidinių KVIS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo

realiu laiku priemonės; šios priemonės automatiškai turi informuoti darbuotojo darbo vietos administratorių apie tai, kuriems kompiuteriams yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

12.6. turi būti operatyviai ištestuojami ir įdiegiami KVIS tvarkytojo darbuotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; KVIS tvarkytojo darbuotojo darbo vietos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie vidinių KVIS tvarkytojo darbuotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

12.7. KVIS sisteminiai administratoriai turi būti perspėjami, kai pagrindinėje KVIS kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

12.8. KVIS administratoriams, pagrindiniam tvarkytojui pateikusiems tiesioginio vadovo patvirtintą prašymą gali būti suteikiama teisė naudoti kompiuterius tiesioginėms pareigoms atlikti ne KVIS tvarkytojo patalpose;

12.9. nuotolinis prisijungimas prie KVIS turi būti vykdomas protokolu, skirtu duomenų šifravimui.

13. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

13.1. KVIS tvarkytojo darbo stotyse ir darbuotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

13.2. programinės įrangos diegimą atlieka tik įgalioti asmenys;

13.3. naudojamos autorizuotos programinės įrangos sąrašą rengia ir reguliariai atnaujina tvarkytojo KVIS sisteminis administratorius;

13.4. neatliekant jokių veiksmų su KVIS 30 minučių, KVIS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis KVIS galima būtų tik pakartotinai patvirtinus savo tapatybę;

13.5. KVIS tarnybinėse stotyse turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti KVIS administratorius apie tai, kuriems KVIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas; KVIS komponentai be kenksmingo programinės įrangos aptikimo priemonių gali būti eksploatuojami tik jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

1.1. turi būti operatyviai ištestuojami ir įdiegiami KVIS tarnybinių stočių įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; KVIS sisteminiai administratoriai reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie KVIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

13.6. pagrindinėse KVIS tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su KVIS funkcionalumu ir administravimu susijusį duomenų srautą;

13.7. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką, kurioje nėra saugomi asmens duomenys.

14. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

14.1. KVIS naudotojas internetu jungiasi prie ugniasiene apsaugotų tarnybinių stočių, naudodamas unikalius identifikacinius prisijungimo duomenis;

14.2. KVIS tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių KVIS naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

14.3. viešaisiais ryšių tinklais perduodamos KVIS elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą ar kitas priemones;

14.4. duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

14.5. duomenų centro ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo ir pažeidimo.

15. Patalpų, kuriose veikia KVIS tarnybinės stotys ir aplinkos saugumo užtikrinimo priemonės:

15.1. KVIS tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

15.2. techninė įranga įnešama ir išnešama iš patalpų tik leidus autorizuotam asmeniui, kuriam pagal atliekamas funkcijas suteikta prieiga prie KVIS tarnybinių stočių;

15.3. KVIS tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

15.4. periodiškai atliekama gaisro gesinimo priemonių patikra;

15.5. svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

15.6. KVIS tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

15.7. įgyvendintos įrangos gamintojų nustatytos techninės įrangos darbo sąlygos;

15.8. visose patalpose, kuriose yra vidinių KVIS naudotojų ir KVIS techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

15.9. patekimas prie vidinių KVIS naudotojų darbo vietų turi būti kontroliuojamas, įrengta elektroninė patalpų perimetro kontrolės sistema;

15.10. tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą;

15.11. įrengta tam tikrų patalpų apsaugos signalizacija, kurios signalai pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai tarnybai;

15.12. sisteminiams administratoriams išduodamos asmeninės magnetinės praėjimo kortelės, kurias jie įeidami ir išeidami pasižymi patikros punktuose; ši informacija saugoma elektronine forma ne trumpiau kaip 1 metus;

15.13. kiti darbuotojai į patalpas patenka tik lydimi administratoriaus arba kito paskirto už patalpų kontrolę asmens;

15.14. įvykus apsaugos sistemos gedimui, pildomas įėjimo punkto žurnalas, nurodant pateikimo priežastį, pradžią ir pabaigą; žurnalas saugomas ne trumpiau kaip 1 metus;

15.15. įvykių žurnalas privalo būti pateiktas saugos įgaliotiniui pareikalavus;

15.16. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

15.17. lankytojai ir svečiai pasirašo įėjimo punkto žurnale. Už apsilankymą atsakingas darbuotojas patvirtina apsilankymo duomenis ir pasirašo įėjimo punkto žurnale;

15.18. į duomenų centrą savarankiškai patekti (pasinaudojant įeigos kortele be rakto) gali tiktai sisteminis administratorius, saugos įgaliotinis ir kiti specialius leidimus turintys darbuotojai, kuriuos patvirtina pagrindinis KVIS tvarkytojas;

15.19. Prieš patenkant į patalpas po 22 val. ir iki 7 val. ir ne darbo dienomis, darbuotojas privalo informuoti saugos tarnybą (apsaugos darbuotoją).

16. KVIS darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

16.1. KVIS tarnybinių stočių įvykių žurnaluose turi būti registruojami ir ne mažiau kaip vienerius metus saugomi duomenys, nurodant įvykio datą ir laiką, apie:

16.1.1. KVIS įjungimą ir išjungimą;

16.1.2. pagrindinių sisteminių komponentų (atminties, procesorių ir duomenų saugyklų bei duomenų bazių) apkrovas, viršijančias nustatytas leistinas reikšmes;

16.1.3. bandymus prieiti prie KVIS administravimo komponentų;

16.1.4. kitus svarbius su KVIS tvarkomos elektroninės informacijos sauga susijusius įvykius pagal suderintą su KVIS sisteminiu administratoriumi ir saugos įgaliotiniu sąrašą.

17. Belaidžio tinklo saugumas ir kontrolė informacinės sistemos tvarkytojo patalpose įgyvendinami pagal kibernetinio saugumo reikalavimų apraše nustatytus informacinės sistemos kategorijai reikalavimus.

18. Svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė:

18.1. svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;

18.2. draudžiama slaptažodžius saugoti programiniame kode;

18.3. turi būti įgyvendinti svetainės kriptografijos reikalavimai:

18.4. svetainės administravimo darbai turi būti atliekami per šifruotą ryšio kanalą, šifruojant ne trumpesniu kaip 256 bitų raktu;

18.5. šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų; sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų;

18.6. svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. Hardware security module);

18.7. draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai;

18.8. turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. Input validation);

18.9. tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;

18.10. tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus;

18.11. turi būti uždrausta naršyti svetainės aplankuose (angl. Directory browsing);

19. Ne rečiau, kaip kartą į metus, atliekamas informacinės sistemos technologinio pažeidžiamumo testavimas.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

20. Saugaus KVIS elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

20.1. asmens duomenys KVIS tvarkomi tik atitinkant teisėto asmens duomenų tvarkymo kriterijus, vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais;

20.2. KVIS duomenis keisti, atnaujinti ir įrašyti gali tik autorizuoti KVIS naudotojai turintys teisę tai atlikti;

20.3. KVIS duomenys teisėtai gali būti naikinami tik turinčių teisę tai atlikti autorizuotų KVIS naudotojų;

20.4. tvarkyti KVIS informacinės sistemos elektroninę informaciją gali tik vidiniai KVIS naudotojai ir KVIS administratoriai, susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų;

20.5. supažindinimas KVIS sistemoje įgyvendinamas užtikrinant susipažinimo įrodomumą;

20.6. visi KVIS naudotojai ir administratoriai privalo saugoti asmens duomenų ir informacijos paslaptį;

20.7. įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

20.8. KVIS duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis KVIS nuostatais ir KVIS duomenų saugos nuostatais;

20.9. už KVIS duomenų saugą pagal kompetenciją atsako KVIS valdytojas, pagrindinis KVIS tvarkytojas ir kiti KVIS tvarkytojai;

20.10. pagrindinio KVIS tvarkytojo ir kitų KVIS tvarkytojų darbuotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams;

20.11. KVIS duomenys KVIS duomenų bazėje saugomi 10 metų nuo paskutinio pakeitimo (papildymo), o suėjus šiam terminui jie yra ištrinami iš KVIS;

20.12. KVIS esantys asmens duomenys KVIS duomenų bazėje saugomi 10 metų nuo paskutinio pakeitimo (papildymo). Pasibaigus saugojimo terminui arba KVIS naudotojui panaikinus savo paskyrą KVIS sistemoje, KVIS naudotojo asmens duomenys per 60 dienų ištrinami iš KVIS.

21. KVIS naudotojų veiksmų registravimo tvarka:

21.1. KVIS naudotojų veiksmai įrašomi automatiniu būdu KVIS duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jame esančių duomenų naudojimo, keitimo, iškraipymo, sunaikinimo;

21.2. KVIS duomenų bazės veiksmų žurnalo įrašai suteikia galimybę nustatyti galimai nesankcionuoto poveikio prisijungimo ir (ar) bandymo prisijungti datą, prisijungimo trukmę, prisijungiančio KVIS naudotojo vardą ir kompiuterio, iš kurio prisijungiama IP adresą ir atliktus veiksmus;

21.3. registruojama informacija apie KVIS naudotojų pasijungimą ir atsijungimą nuo KVIS, taip pat ir nesėkmingus bandymus registruotis į KVIS;

21.4. registruojama informacija apie KVIS naudotojų vykdomus elektroninės informacijos tvarkymo veiksmus (informacijos įvedimą, keitimą, atnaujinimą, panaikinimą);

21.5. šie duomenys turi būti kopijuojami ir saugomi ne toje pačioje tarnybinėje stotyje, kurioje jie buvo sukurti;

21.6. šie duomenys turi būti analizuojami ne rečiau kaip kartą per savaitę;

21.7. šie duomenys pagrindiniame įvykių žurnale turi būti saugomi ne trumpiau kaip 30 dienų, o kopijoje turi būti saugomi ne trumpiau kaip 1 metus;

21.8. KVIS duomenų bazės veiksmų žurnalo duomenys prieinami atitinkamas teises turintiems KVIS naudotojams (KVIS sisteminiam administratoriui ir saugos įgaliotiniui).

22. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

22.1. už KVIS elektroninės informacijos atsarginių kopijų darymą yra atsakingas KVIS sisteminis administratorius;

22.2. prarasti, iškraipyti ar sunaikinti KVIS duomenys atkuriami iš KVIS duomenų atsarginių kopijų;

22.3. KVIS duomenų bazių ir archyvų valdymas organizuojamas atsižvelgiant į KVIS nuostatų 36-37 punktų reikalavimus;

22.4. pilna KVIS duomenų kopija daroma ne rečiau kaip kartą per savaitę, pokyčių (inkrementinė kopija) – ne rečiau kaip kartą per parą;

22.5. pilnos duomenų kopijos saugomos ne trumpiau kaip vieną mėnesį, pokyčių – ne trumpiau kaip vieną savaitę;

22.6. duomenų kopijos saugomos kitoje patalpoje nuo pagrindinių KVIS tarnybinių stočių;

22.7. duomenis, atstatyti iš atsarginės kopijos turi teisę KVIS sisteminis administratorius, prieš tai įsitikinęs kad toks atstatymas nesugadins esamų duomenų;

22.8. apie planuojamą duomenų atstatymą ir jį įvykdžius sisteminis administratorius privalo informuoti saugos įgaliotinį;

22.9. visiški KVIS elektroninės informacijos atkūrimo bandymai vykdomi vieną kartą per metus;

22.10. visiški KVIS elektroninės informacijos atkūrimo bandymai vykdomi ne darbo valandomis ir prieš tai informavus visus KVIS naudotojus;

22.11. už visiškus KVIS atkūrimo bandymus yra atsakingas KVIS sisteminis administratorius. Elektroninės informacijos atkūrimo bandymų metodai nustatomi veiklos tęstinumo plane.

23. Elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms ir elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

23.1. KVIS elektroninė informacija yra teikiama institucijoms, kitiems juridiniams ir fiziniams asmenims, kai Lietuvos Respublikos įstatymai ir (ar) Europos Sąjungos teisės aktai nenustato kitaip;

23.2. KVIS tvarkomi duomenys teikiami ir naudojami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais;

23.3. KVIS duomenys teikiami suteikiant galimybę leidžiamosios kreipties būdu peržiūrėti juos internetu ar kitais elektroninių ryšių tinklais;

23.4. KVIS interneto svetainėje (portale) viešinamos absolventų karjeros stebėsenos ataskaitos, kuriose teikiami nuasmeninti absolventų karjeros stebėsenos duomenys;

23.5. duomenų mainai tarp KVIS ir susijusių registrų bei kitų informacinių sistemų vykdomi su šių registrų ir informacinių sistemų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, terminais ir numatyta apimtimi;

23.6. tretiesiems asmenims, turintiems teisę pagal Lietuvos Respublikos teisės aktus gauti duomenis, šie duomenys teikiami pagal prašymus, kuriuose nurodomas duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, teikiamų duomenų apimtis, (vienkartinio prašymo atveju) arba duomenų teikimo sutartis (daugkartinio prašymo atveju), kuriose turi būti nurodomas duomenų teikimo teisinis pagrindas, teikiamų duomenų apimtis, naudojimo tikslas, sąlygos ir tvarka;

23.7. duomenys duomenų gavėjams teikiami tokio turinio ir tokios formos, kurie institucijoje jau naudojami ir nereikalingi papildomo duomenų apdorojimo;

23.8. duomenys sistemos nuostatuose patvirtintiems duomenų gavėjams teikiami neatlygintinai, išskyrus atvejus, kai reikalingas papildomas duomenų apdorojimas arba darbai atliekami skubos tvarka;

23.9. duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka;

23.10. už KVIS elektroninės informacijos perkėlimą iš susijusių registrų ir kitų informacinių sistemų bei, poreikiui esant, elektroninės informacijos teikimas kitoms informacinėms sistemoms yra atsakingas KVIS taikomosios programinės įrangos administratorius.

24. Apsaugos nuo informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo tvarka:

24.1. KVIS sisteminis administratorius, užtikrindamas KVIS duomenų vientisumą, privalo naudoti visas technines, programines ir administracines priemones, skirtas KVIS ir joje saugomiems, apdorojamiems duomenims apsaugoti nuo neteisėtų veiksmų;

24.2. KVIS naudotojas, įtaręs, kad su KVIS duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai savo institucijos darbo vietos administratoriui;

24.3. institucijos darbo vietos administratorius jam prieinamomis programinėmis priemonėmis patikrina gautą pranešimą apie saugos pažeidimą ir, faktui pasitvirtinus, imasi visų įmanomų prevencinių veiksmų;

24.4. apie pažeidimo faktą, atliktus veiksmus pažeidimo pasekmių likvidavimui ir jo pasikartojimo prevencijai bei siūlomas papildomas priemones darbo vietos administratorius informuoja pagrindinio tvarkytojo KVIS taikomosios įrangos administratorių ir KVIS saugos įgaliotinį;

24.5. KVIS saugos įgaliotinis, gavęs pranešimą apie vykdomus galimai neteisėtus veiksmus su KVIS arba su KVIS tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras.

25. KVIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

25.1. techninės, programinės ir sisteminės įrangos naujinimui galioja pokyčių valdymo tvarka;

25.2. KVIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, kuriai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastuktūros priežiūros funkcijos (toliau – paslaugų teikėjas), priklausomai nuo konkretaus atvejo, derina pagrindinio tvarkytojo KVIS taikomosios įrangos ir KVIS sisteminis administratorius arba ji aprašoma paslaugų, susijusių su KVIS programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

26. KVIS pokyčių valdymo tvarka:

26.1. KVIS valdytojas užtikrina informacinės sistemos pokyčių (toliau – pokyčiai) valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą

(administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas) pokyčių prioritetų nustatymo (eiliškumas) procesus;

26.2. pokyčiai identifikuojami nustačius KVIS naudotojų, administratorių, ir kitų rolių poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardinamais atvejais;

26.3. pokyčius turi teisę inicijuoti duomenų valdymo įgaliotinis, saugos įgaliotinis ar administratorius, o įgyvendinti – sisteminis administratorius;

26.4. visi potencialūs pokyčiai registruojami pokyčių registre, įvertinus ir valdytojui patvirtinus įtakos vertinimą ir prioritetą;

26.5. kibernetiniam saugumui užtikrinti naudojamų priemonių diegimas ir šių priemonių parametrų keitimas laikomas pokyčiu ir atliekamas vadovaujantis ta pačia tvarka;

26.6. KVIS taikomosios programinės įrangos pokyčiai atliekami tik įvertinus pokyčio poreikį, pokyčio apimtį ir suderinus sistemos modernizavimo mastą;

26.7. KVIS sistemos funkcijų ir galimybių sąrankos aprašai turi būti nuolat atnaujinami ir atitikti esamą informacinės sistemos sąrankos būklę;

26.8. pokyčiai įgyvendinami valdytojo patvirtintu eiliškumu, atsižvelgiant į sutartą svarbumą ir skubumą;

26.9. visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su informacinės sistemos pagrindiniu tvarkytoju bei duomenų valdymo įgaliotiniu;

26.10. prieš atlikdamas KVIS pokyčius, kurių metu gali iškilti grėsmė duomenų ir KVIS konfidencialumui, vientisumui ar pasiekiamumui, KVIS sisteminis administratorius privalo planuojamus KVIS pokyčius ištestuoti bandomojoje aplinkoje;

26.11. programinės įrangos testavimas atliekamas naudojant atskirą tam skirtą testavimo aplinką, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos;

26.12. atlikęs vykdomų KVIS pokyčių testavimą, KVIS sisteminis administratorius gali pradėti įgyvendinti KVIS pokyčius tik gavęs patvirtinimą ir suderinęs pokyčio diegimo grafiką su sistemos valdytoju;

26.13. planuodamas KVIS pokyčius, kurių metu galimi KVIS veikimo sutrikimai, KVIS sisteminis administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki KVIS pokyčių vykdymo pradžios elektroniniu paštu informuoti KVIS duomenų valdymo ir saugos įgaliotinius, kitus administratorius ir elektroniniu būdu sistemoje informuoti vidinius KVIS naudotojus apie tokių darbų pradžią ir galimus KVIS veikimo sutrikimus.

27. Vidinių KVIS naudotojų pareigoms atlikti naudojamų nešiojamų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

27.1. vidinių KVIS naudotojų administravimo poreikiams naudojamiems nešiojamiems kompiuteriams ir mobiliems įrenginiams taikomi šie papildomi reikalavimai:

27.1.1. išvežti iš patalpų nešiojamieji kompiuteriai ir mobilieji įrenginiai negali būti palikti be priežiūros viešose vietose;

27.1.2. kelionės metu nešiojamieji KVIS sisteminių administratorių kompiuteriai turi būti saugomi ir rakinami fizinei apsaugai skirtomis priemonėmis;

27.1.3. Visų KVIS administratorių nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti apsaugoti slaptažodžiais, sudėtingumu atitinkančiais ne mažiau kaip KVIS naudotojų administravimo taisyklių reikalavimus.

28. Saugaus interneto paslaugų ir elektroninio pašto naudojimo tvarka:

28.1. Saugaus interneto paslaugų ir elektroninio pašto naudojimo reikalavimai sistemos naudotojams nustatyti Lietuvos mokslo ir studijų institucijų kompiuterių tinklo LITNET naudojimo taisyklėse, patvirtintose 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“.

IV SKYRIUS
REIKALAVIMAI, KELIAMI KVIS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

29. Perkant paslaugas, darbus ar įrangą, susijusius su infrastruktūra, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi būti iš anksto nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, reikalavimams.

30. Reikalavimai KVIS funkcionuoti reikalingoms paslaugų teikėjų teikiamoms paslaugoms nustatomi šių paslaugų teikimo sutartyse.

31. Paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja KVIS taikomąją programinę įrangą, naudodamas:

31.1. įgyvendintas elektroninės informacijos saugos nuo nesankcionuoto poveikio sisteminei, programinei įrangai ir patalpoms priemones;

31.2. KVIS testinės duomenų bazės duomenis (KVIS taikomajai programinei įrangai modifikuoti);

31.3. tik legalią sisteminę programinę įrangą.

32. Paslaugų teikėjų prieigos prie KVIS lygiai ir sąlygos:

32.1. Pagrindinio tvarkytojo KVIS administratorius suteikia prieigos prie KVIS duomenų teisę (peržiūrėti KVIS duomenis, atlikti užklausas KVIS, vykdyti veiksmus su KVIS duomenimis ir kt.), o pagrindinio tvarkytojo KVIS sisteminis administratorius suteikia fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti;

32.2. Pagrindinio tvarkytojo KVIS administratorius, suteikdamas prieigos prie KVIS duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie KVIS duomenų sąlygomis;

32.3. pasibaigus sutartyje nurodytam laikotarpiui, pagrindinio tvarkytojo KVIS administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie KVIS duomenų teisę ir apie tai jį informuoja.

33. Visi KVIS administratoriai ir naudotojai, pažeidę šių taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.