PATVIRTINTA
Vilniaus universiteto rektoriaus
2015 m. birželio 26 d.
įsakymu Nr. R-254

VILNIAUS UNIVERSITETO STUDIJŲ INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Vilniaus universiteto studijų informacinės sistemos (toliau – VUSIS) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Tvarkymo taisyklės) tikslas – nustatyti VUSIS tvarkytojo, VUSIS administratorių, VUSIS duomenų saugos įgaliotinio, kitų VUSIS tvarkytojų ir VUSIS naudotojų veiksmus, užtikrinančius saugų VUSIS techninės ir programinės įrangos funkcionavimą, VUSIS duomenų tvarkymą ir teikimą VUSIS duomenų gavėjams.

2. VUSIS saugaus elektroninės informacijos tvarkymo taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu, Nr. 1V-832, Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) (toliau – Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms), reikalavimais, VUSIS nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2009 m. sausio 8 d. įsakymu R-7, VUSIS duomenų saugos nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2014 m. lapkričio 10 d. įsakymu R-512, taip pat kitais teisės aktais ir standartais, reglamentuojančiais duomenų tvarkymo teisėtumą, tvarkytojų veiklą ir duomenų saugos valdymą.

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

4. Visi VUSIS naudotojai ir administratoriai, VUSIS duomenų valdymo ir VUSIS duomenų saugos įgaliotinis susipažįsta ir sutinka su šiomis taisyklėmis elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

5. VUSIS saugaus elektroninės informacijos tvarkymo taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, VUSIS nuostatuose, VUSIS duomenų saugos nuostatuose ir kituose teisės aktuose bei saugų duomenų tvarkymą reglamentuojančiuose standartuose. Taisyklėse naudojamos papildomai apibrėžiamos sąvokos:

5.1. sisteminis administratorius – tai informacinės sistemos administratorius, prižiūrintis sistemos infrastruktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą;

5.2. darbo vietų administratorius– administratorius, atsakingas už padalinio kompiuterinių darbo vietų, įdiegtos programinės įrangos ir lokalaus tinklo priežiūrą.

6. VUSIS tvarkomos elektroninės informacijos struktūra pateikiama Vilniaus universiteto rektoriaus Vilniaus universiteto rektoriaus 2009 m. sausio 8 d. įsakymu R-7 patvirtintų VUSIS nuostatų III skyriuje.

7. VUSIS tvarkoma informacija yra skirstoma į šias grupes:

7.1. VUSIS administratorių tvarkoma informacija;

7.2. VUSIS naudotojų tvarkoma informacija.

8.VUSIS pagrindinis administratorius atsakingas už šios informacijos tvarkymą:

8.1. naudotojų prisijungimo duomenys;

8.2. naudotojų rolės;

8.3. naudotojų teisės;

8.4. klasifikatoriai (VUSIS nuostatų III skyriaus 19.9).

9.VUSIS padalinio administratorius atsakingas už šios informacijos tvarkymą:

9.1. studentų asmens duomenys (įskaitant VUSIS nuostatuose išvardintus duomenis apie asmens tapatybę, išsilavinimą ir studijas);

9.2. išmokų ir įmokų duomenys;

9.3. studijų programų ir dalykų aprašai.

10. VUSIS duomenų bazės administratorius atsakingas už šios informacijos tvarkymą:

10.1. teikiami registrams duomenys;

10.2. teikiami kitoms institucijoms duomenys;

10.3. duomenų teikimo aprašai;

10.4. duomenų teikimo paslaugų stebėsenos duomenys;

10.5. naudotojų duomenų tvarkymo stebėsenos duomenys.

11. Kiti VUSIS naudotojai atsakingi už šios informacijos tvarkymą:

11.1. studentai:

11.1.1. studento nurodyta asmens kontaktinė informacija;

11.1.2. studento registracija į dalykus;

11.2. dėstytojai:

11.2.1. studento studijų rezultatai;

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

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

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

12.2. informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei trečios kategorijos informacinės sistemos – 16 val.

13. Kompiuterinės įrangos saugos priemonės:

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

13.2. VUSIS administratorių ir vidinių VUSIS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti darbo vietų administratorių apie tai, kuriems kompiuteriams yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

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

13.4. VUSIS sisteminiai administratoriai turi būti perspėjami, kai pagrindinėje VUSIS kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio

atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

13.5. VUSIS padalinių administratoriams, pagrindiniam administratoriui pateikusiems tiesioginio vadovo patvirtintą prašymą, gali būti suteikiama teisė naudoti kompiuterius tiesioginėms pareigoms atlikti ne VUSIS tvarkytojo patalpose;

13.6. nuotolinis prisijungimas prie VUSIS turi būti vykdomas protokolu, skirtu duomenų šifravimui.

14. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

14.1. VUSIS darbo stotyse ir vidinių naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

14.2. vidinių naudotojų kompiuterinėje įrangoje naudojamos autorizuotos programinės įrangos sąrašą rengia ir reguliariai atnaujina VUSIS pagrindinis administratorius;

14.3. VUSIS tarnybinių stočių techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

14.4. VUSIS tarnybinių stočių techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

14.5. programinę įrangą turi diegti tik VUSIS tvarkytojo vadovo įgalioti asmenys;

14.6. neatliekant jokių veiksmų su VUSIS 15 minučių, VUSIS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis VUSIS galima būtų tik pakartotinai patvirtinus savo tapatybę;

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

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

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

14.10. VUSIS programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms 14.8 punkto reikalavimais.

15. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

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

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

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

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

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

16. Patalpų, kuriose veikia VUSIS tarnybinės stotys ir aplinkos saugumo užtikrinimo priemonės:

16.1. VUSIS tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

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

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

16.4. periodiškai atliekama gaisro gesinimo priemonių patikra;

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

16.6. VUSIS tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

16.7. įgyvendintos įrangos gamintojų nustatytos techninės įrangos darbo sąlygos;

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

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

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

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

16.12. 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;

16.13. kiti darbuotojai į patalpas patenka tik lydimi VUSIS sisteminio administratoriaus arba paskirto už patalpų kontrolę asmens;

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

16.15. įvykių žurnalas privalo būti pateiktas duomenų saugos įgaliotiniui pareikalavus;

16.16. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

16.17. Už apsilankymą atsakingas darbuotojas registruoja lankytojų ir svečių apsilankymo duomenis ir pasirašo įėjimo punkto žurnale;

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

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

17. VUSIS darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

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

17.1.1. VUSIS įjungimą ir išjungimą;

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

17.1.3. bandymus prieiti prie VUSIS administravimo komponentų;

17.1.4. kitus svarbius su VUSIS tvarkomos elektroninės informacijos sauga susijusius įvykius pagal suderintą su VUSIS sisteminiu administratoriumi ir duomenų saugos įgaliotiniu sąrašą.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

18. Saugaus VUSIS elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

18.1. asmens duomenys VUSIS tvarkomi tik atitinkant teisėto asmens duomenų tvarkymo kriterijus, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pagrindais;

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

18.3. VUSIS duomenys teisėtai gali būti naikinami tik autorizuotų VUSIS naudotojų, turinčių teisę tai atlikti;

18.4. visi VUSIS naudotojai ir administratoriai privalo saugoti asmens duomenų ir informacijos paslaptį;

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

18.6. VUSIS duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis VUSIS nuostatais ir VUSIS duomenų saugos nuostatais;

18.7. už VUSIS duomenų saugą pagal kompetenciją Lietuvos Respublikos įstatymų nustatyta tvarka atsako VUSIS valdytojas ir VUSIS tvarkytojas;

18.8. visi VUSIS naudotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja ir perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams;

18.9. VUSIS asmens duomenų saugumas užtikrinamas vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms.

19. VUSIS naudotojų veiksmų registravimo tvarka:

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

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

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

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

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

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

19.7. VUSIS duomenų bazės veiksmų žurnalo duomenys prieinami atitinkamas teises turintiems VUSIS naudotojams (VUSIS duomenų bazės administratoriui ir duomenų saugos įgaliotiniui).

20. Atsarginių elektroninės informacijos kopijų darymo ir saugojimo tvarka nustatoma VUSIS tvarkytojo direktoriaus įsakymu.

21. Elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka nustatoma VUSIS tvarkytojo direktoriaus įsakymu.

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

22.1. VUSIS elektroninė informacija institucijoms, kitiems juridiniams ir fiziniams asmenims teikiama vadovaujantis Studijuojančiųjų asmens duomenų tvarkymo Vilniaus universitete taisyklėmis;

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

22.3. duomenų mainai tarp VUSIS 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;

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

22.5. 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;

22.6. už VUSIS elektroninės informacijos perdavimą į registrus ir kitas informacines sistemas bei gavimą iš jų yra atsakingas VUSIS tvarkytojas.

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

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

23.2. VUSIS naudotojas, įtaręs, kad su VUSIS duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai savo padalinio darbo vietų administratoriui;

23.3. padalinio darbo vietų administratorius jam prieinamomis programinėmis priemonėmis patikrina gautą pranešimą apie saugos pažeidimą ir, faktui pasitvirtinus, imasi visų įmanomų prevencinių veiksmų;

23.4. apie pažeidimo faktą, atliktus veiksmus pažeidimo pasekmių likvidavimui ir jo pasikartojimo prevencijai bei siūlomas papildomas priemones darbo vietų administratorius informuoja pagrindinį administratorių;

23.5. VUSIS duomenų saugos įgaliotinis, gavęs pranešimą apie vykdomus galimai neteisėtus veiksmus su VUSIS arba su VUSIS tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento tyrimą.

24. VUSIS programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

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

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

25. VUSIS pokyčių valdymo tvarka:

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

25.2. VUSIS 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;

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

25.4. pokyčius turi teisę inicijuoti VUSIS duomenų valdymo įgaliotinis, duomenų saugos įgaliotinis ar administratorius, o įgyvendinti – duomenų bazės administratorius;

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

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

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

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

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

25.10. prieš atlikdamas VUSIS pokyčius, kurių metu gali iškilti grėsmė duomenų ir VUSIS konfidencialumui, vientisumui ar pasiekiamumui, VUSIS duomenų bazės administratorius privalo planuojamus VUSIS pokyčius ištestuoti bandomojoje aplinkoje;

25.11. programinės įrangos testavimas atliekamas imantis elektroninės informacijos saugos priemonių, numatytų šios tvarkos punkte 14.10;

25.12. atlikęs vykdomų VUSIS pokyčių testavimą, VUSIS duomenų bazės administratorius gali pradėti įgyvendinti VUSIS pokyčius tik gavęs patvirtinimą ir suderinęs pokyčio diegimo grafiką su VUSIS valdytoju;

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

26. Vidinių VUSIS naudotojų pareigoms atlikti naudojamų nešiojamų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

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

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

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

26.1.3. Visų VUSIS administratorių nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti apsaugoti slaptažodžiais, sudėtingumu atitinkančiais ne mažiau kaip šių taisyklių reikalavimus.

IV. REIKALAVIMAI, KELIAMI VUSIS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

27. Reikalavimai VUSIS funkcionuoti reikalingoms paslaugų teikėjų teikiamoms paslaugoms nustatomi šių paslaugų teikimo sutartyse.

28. Paslaugų teikėjų prieigos prie VUSIS lygiai ir sąlygos:

28.1. VUSIS pagrindinis administratorius suteikia prieigos prie VUSIS duomenų teisę (peržiūrėti VUSIS duomenis, atlikti užklausas VUSIS, vykdyti veiksmus su VUSIS duomenimis ir kt.), o VUSIS duomenų bazės administratorius suteikia fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti;

28.2. VUSIS pagrindinis administratorius, suteikdamas prieigos prie VUSIS duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie VUSIS duomenų sąlygomis;

28.3. pasibaigus sutartyje nurodytam laikotarpiui, VUSIS pagrindinis administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie VUSIS duomenų teisę ir apie tai jį informuoja.

29. Reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklais ir kitoms paslaugoms:

29.1. užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas;

29.2. užtikrinamas tik įgaliotų asmenų patekimas į atitinkamas patalpas;

29.3. Paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas:

29.3.1. kuria ar modifikuoja VUSIS taikomąją programinę įrangą, naudodamas įgyvendintas elektroninės informacijos saugos nuo nesankcionuoto poveikio sisteminei, programinei įrangai ir patalpoms priemones;

29.3.2. VUSIS testavimo duomenų bazės duomenis;

29.3.3. VUSIS kūrimui ir testavimui skirtą infrastruktūrą;

29.3.4. prisijungimui nuotoliniu būdu prie VUSIS aplinkų laikosi VUSIS duomenų saugos nuostatuose keliamų reikalavimų;

29.3.5. darbui naudoja tik legalią sisteminę programinę įrangą;

29.3.6. laikosi šių taisyklių, VUSIS duomenų saugos nuostatų ir VUSIS naudotojų administravimo taisyklėse nustatytų pareigų VUSIS administratoriams ir vidiniams naudotojams.

30. VUSIS tvarkytojas, VUSIS duomenų valdymo ir duomenų saugos įgaliotinis, VUSIS administratoriai ir naudotojai, pažeidę šių taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____