PATVIRTINTA
Vilniaus universiteto rektoriaus
2012 m. balandžio 18 d. įsakymu Nr. R-155
(Vilniaus universiteto rektoriaus
2018 m. spalio 26 d. įsakymo Nr. R-580
redakcija)

VIRTUALI ISTORINĖ LIETUVA: LDK INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Virtuali istorinė Lietuva: LDK informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato Virtuali istorinė Lietuva: LDK informacinės sistemos (toliau – informacinė sistema) tvarkytojo, jo paskirtų informacinės sistemos administratorių, informacinės sistemos saugos įgaliotinio ir informacinės sistemos naudotojų atsakomybę bei veiksmus, užtikrinančius saugų informacinės sistemos techninės ir programinės įrangos funkcionavimą, informacinės sistemos duomenų tvarkymą ir teikimą informacinės sistemos duomenų teikėjams.

2. Taisyklės parengtos vadovaujantis Bendruoju 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Virtuali istorinė Lietuva: LDK informacinės sistemos nuostatais (toliau – Informacinės sistemos nuostatai) ir Virtuali istorinė Lietuva: LDK duomenų saugos nuostatais (toliau – Informacinės sistemos duomenų saugos nuostatai), patvirtintais Vilniaus universiteto rektoriaus 2012 m. balandžio 18 d. įsakymu Nr. R-155 „Dėl Virtuali istorinė Lietuva: LDK informacinės sistemos nuostatų ir Virtuali istorinė Lietuva: LDK informacinės sistemos duomenų saugos nuostatų patvirtinimo“, taip pat kitais teisės aktais ir standartais, reglamentuojančiais duomenų tvarkymo teisėtumą, tvarkytojų veiklą ir duomenų saugos valdymą.

3. Taisyklės taikomos informacinės sistemos valdytojui ir informacinės sistemos tvarkytojui, informacinės sistemos saugos įgaliotiniui, visiems informacinės sistemos naudotojams ir administratoriams.

4. Taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos informacinės sistemos nuostatuose, ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

5. Informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių) sąrašas pateikiamas Informacinės sistemos nuostatų IV skyriaus 16 punkte.

6. Informacinėje sistemoje tvarkoma informacija yra skirstoma į šias grupes:

6.1. Naudotojų tvarkoma informacija;

6.2. Ekspertų tvarkoma informacija;

6.3. Administratorių tvarkoma informacija.

7. Visi naudotojai gali vykdyti paieškas, peržiūrėti informaciją, nurodytą Informacinės sistemos nuostatų IV skyriaus 16.2-16.3 punktuose;

8. Vidiniai naudotojai (ekspertai) gali:

8.1. vykdyti ir išsaugoti paieškas, peržiūrėti informaciją, nurodytą informacinės sistemos nuostatų IV skyriaus 16.2-16.3 punktuose;

8.2. kurti ir keisti savo profilio duomenis (informacinės sistemos nuostatų IV skyriaus 16.1.1 punktas);

9. Vidiniai naudotojai (ekspertai) gali:

9.1. vykdyti paieškas, peržiūrėti ir keisti informaciją, nurodytą informacinės sistemos nuostatų IV skyriaus 16.2-16.5 punktuose;

9.2. kurti ir keisti savo profilio duomenis (informacinės sistemos nuostatų IV skyriaus 16.1.2 punktas).

10. Administratoriai yra atsakingi už šios informacijos tvarkymą:

10.1. naudotojų duomenys, vaidmenys ir teisės;

10.2. paslaugų iniciavimo ir teikimo duomenys:

10.2.1. paslaugų teikimą aprašantys duomenys;

10.2.2. duomenų gavimas iš Virtualios kultūros paveldo informacinės sistemos (toliau – VEPIS), numatytas informacinės sistemos nuostatų IV skyriaus 17 punkte;

10.2.3. duomenų teikimas į VEPIS, numatytas informacinės sistemos nuostatų IV skyriaus 18 punkte;

10.3. paslaugų teikimo stebėsenos duomenys:

10.3.1. duomenų užklausimo laikas;

10.3.2. duomenų perdavimo laikas;

10.3.3. paslaugų suteikimo laikas;

10.3.4. kiti techniniai duomenys paslaugų teikimo stebėsenai atlikti.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

11. Saugiam informacinės sistemos elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės, kurios užtikrintų:

11.1. kad informacinės sistemos prieinamumas būtų ne mažiau kaip 70 proc. laiko per metus darbo metu darbo dienomis;

11.2. kad informacinės sistemos neveikimo laikotarpis nebūtų ilgesnis nei (ketvirtos kategorijos informacinės sistemos) – 24 val.;

12. Kompiuterinės įrangos saugos priemonės:

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

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

12.3. kompiuterinės įrangos gedimų registravimas vykdomas elektroniniame kompiuterinės įrangos gedimų žurnale;

12.4. informacinės sistemos administratorių ir vidinių 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;

12.5. turi būti operatyviai ištestuojami ir įdiegiami informacinės sistemos tvarkytojo darbuotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

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

12.7. informacinės sistemos administratoriams, informacinės sistemos saugos įgaliotiniui pateikusiems tiesioginio vadovo patvirtintą prašymą gali būti suteikiama teisė naudoti kompiuterius tiesioginėms pareigoms atlikti ne informacinės sistemos tvarkytojo patalpose;

12.8. nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas protokolu, skirtu duomenų šifravimui.

13. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

13.1. informacinės sistemos 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 (ne rečiau kaip kartą metuose) atnaujina informacinės sistemos administratorius;

13.4. neatliekant jokių veiksmų su informacinės sistemos 30 minučių, darbo vietos įranga turi užsirakinti, kad toliau naudotis informacinės sistemos galima būtų tik pakartotinai patvirtinus savo tapatybę;

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

13.6. turi būti operatyviai ištestuojami ir įdiegiami informacinės sistemos tarnybinių stočių įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; informacinės sistemos administratoriai turi nuolat vertinti informaciją apie informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumus;

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

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

14. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

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

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

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

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

15.1. informacinės sistemos 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 informacinės sistemos tarnybinių stočių;

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

15.4. informacinės sistemos tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

15.5. įvykus sistemos gedimui, pildomas elektroninis žurnalas, nurodant priežastį, pradžią ir pabaigą;

15.6. elektroninis žurnalas privalo būti pateiktas informacinės sistemos saugos įgaliotiniui pareikalavus;

15.7. duomenų centro lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

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

15.9. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

16. Saugaus informacinės sistemos elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

16.1. informacinės sistemos duomenis keisti, atnaujinti, įrašyti ir naikinti gali tik autorizuoti informacinės sistemos naudotojai;

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

16.3. supažindinimas informacinės sistemos sistemoje įgyvendinamas užtikrinant susipažinimo įrodomumą;

16.4. visi informacinės sistemos naudotojai ir administratoriai, pažeidę saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka;

16.5. visi informacinės sistemos naudotojai ir administratoriai privalo saugoti asmens duomenų ir informacijos paslaptį;

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

16.7. informacinės sistemos duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis Informacinės sistemos nuostatais ir Informacinės sistemos duomenų saugos nuostatais;

16.8. už informacinės sistemos duomenų saugą pagal kompetenciją Lietuvos Respublikos įstatymų nustatyta tvarka atsako informacinės sistemos valdytojas ir tvarkytojas;

16.9. informacinės sistemos tvarkytojo 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;

16.10. informacinės sistemos duomenys informacinės sistemos duomenų bazėje saugomi neterminuotai;

16.11. informacinėje sistemoje tvarkomi asmens duomenys informacinės sistemos duomenų bazėje saugomi terminais, nurodytais Informacinės sistemos nuostatuose. Pasibaigus saugojimo terminui arba informacinės sistemos naudotojui panaikinus savo paskyrą informacinės sistemos sistemoje, informacinės sistemos naudotojo asmens duomenys per metus ištrinami iš informacinės sistemos;

16.12. informacinės sistemos asmens duomenų saugumas užtikrinamas vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, 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, juos įgyvendinančiais Lietuvos Respublikos ir Universiteto teisės aktais..

17. Informacinės sistemos naudotojų veiksmų registravimo tvarka:

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

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

17.3. registruojama informacija apie informacinės sistemos naudotojų pasijungimą ir atsijungimą nuo informacinės sistemos, taip pat ir nesėkmingus bandymus registruotis į informacinę sistemą;

17.4. registruojama informacija apie informacinės sistemos naudotojų vykdomus elektroninės informacijos tvarkymo veiksmus (informacijos įvedimą, keitimą, atnaujinimą, panaikinimą);

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

17.6. informacinės sistemos duomenų bazės veiksmų žurnalo duomenys prieinami atitinkamas teises turintiems informacinės sistemos naudotojams (informacinės sistemos sisteminiam administratoriui ir saugos įgaliotiniui).

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

18.1. už informacinės sistemos elektroninės informacijos atsarginių kopijų darymą yra atsakingas informacinės sistemos tvarkytojo paskirtas administratorius;

18.2. prarasti, iškraipyti ar sunaikinti informacinės sistemos duomenys atkuriami iš informacinės sistemos duomenų atsarginių kopijų;

18.3. informacinės sistemos duomenų bazių ir archyvų valdymas organizuojamas atsižvelgiant į Informacinės sistemos nuostatų 26-27 punktų reikalavimus;

18.4. pilna informacinės sistemos duomenų kopija daroma ne rečiau kaip kartą per savaitę, pokyčių (inkrementinė kopija) – ne rečiau kaip kartą per parą;

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

18.6. duomenų kopijos saugomos kitoje patalpoje nuo pagrindinių informacinės sistemos tarnybinių stočių;

18.7. duomenis, atstatyti iš atsarginės kopijos turi teisę tik informacinės sistemos tvarkytojo paskirtas informacinės sistemos administratorius, prieš tai įsitikinęs kad toks atstatymas nesugadins esamų duomenų;

18.8. apie planuojamą duomenų atstatymą ir jį įvykdžius informacinės sistemos administratorius privalo informuoti informacinės sistemos saugos įgaliotinį;

18.9. visiški informacinės sistemos elektroninės informacijos atkūrimo bandymai vykdomi vieną kartą per metus;

18.10. visiški informacinės sistemos elektroninės informacijos atkūrimo bandymai vykdomi ne darbo valandomis, iš anksto informavus visus informacinės sistemos naudotojus;

18.11. už visiškus informacinės sistemos atkūrimo bandymus atsako informacinės sistemos tvarkytojo paskirtas informacinės sistemos infrastruktūrą prižiūrintis administratorius. Elektroninės informacijos atkūrimo bandymų metodai nustatomi veiklos tęstinumo plane.

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

19.1. informacinės sistemos elektroninė informacija yra teikiama duomenų gavėjams;

19.2. informacinės sistemos tvarkomi asmens duomenys teikiami ir naudojami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais;

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

19.4. informacinės sistemos interneto svetainėje (portale) viešinami Informacinės sistemos nuostatų 16.2-16.3 punktuose nurodyti duomenys;

19.5. duomenų mainai tarp informacinės sistemos ir susijusių informacinių sistemų vykdomi sutartiniais pagrindais, numatytu specifikacijoje būdu ir tvarka;

19.6. tretiesiems asmenims, turintiems teisę pagal Lietuvos Respublikos teisės aktus gauti sistemoje tvarkomus duomenis, šie duomenys teikiami pagal vienkartinius 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;

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

19.8. Informacinės sistemos nuostatuose nurodytiems duomenų gavėjams duomenys teikiami neatlygintinai;

19.9. 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.

19.10. už informacinės sistemos elektroninės informacijos perkėlimą iš susijusių informacinių sistemų bei, poreikiui esant, elektroninės informacijos teikimą kitoms informacinėms sistemoms yra atsakingas tvarkytojo paskirtas informacinės sistemos administratorius;

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

20.1. informacinės sistemos administratoriai, užtikrindami informacinės sistemos duomenų vientisumą, privalo naudoti visas technines, programines ir administracines priemones, skirtas informacinės sistemos ir joje saugomiems, apdorojamiems duomenims apsaugoti nuo neteisėtų veiksmų;

20.2. informacinės sistemos naudotojas, įtaręs, kad su informacinės sistemos duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai administratoriui, atsakingam už informacinės sistemos naudotojo darbo vietą;

20.3. administratorius, atsakingas už informacinės sistemos naudotojo darbo vietą, jam prieinamomis programinėmis priemonėmis, patikrina gautą pranešimą apie saugos pažeidimą ir, faktui pasitvirtinus, informuoja informacinės sistemos administratorių ir informacinės sistemos saugos įgaliotinį bei imasi visų įmanomų prevencinių veiksmų.

20.4. Informacinės sistemos administratorius išanalizuoja gautą informaciją, įvertina, ar nereikėtų papildomų prevencinių priemonių;

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

21. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

21.1. informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka su trečiąja šalimi, jei 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), aprašoma paslaugų,

susijusių su informacinės sistemos programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

22. Techninės, programinės ir sisteminės įrangos naujinimui galioja ši pokyčių valdymo tvarka:

22.1. informacinės sistemos 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, skubumas, apimtis ir sąnaudos) pokyčių prioritetų nustatymo (eiliškumas) procesus;

22.2. pokyčiai identifikuojami nustačius informacinės sistemos naudotojų, administratorių, ir kitų rolių poreikius, apibendrinus kylančias priežiūros problemas, galimą naudą valdytojo funkcijų atlikimui ir kitais gerosios praktikos įvardinamais atvejais;

22.3. pokyčius turi teisę inicijuoti duomenų valdymo įgaliotinis, informacinės sistemos saugos įgaliotinis ar informacinės sistemos administratorius, o įgyvendinti – informacinės sistemos administratorius;

22.4. sprendimą dėl informacinės sistemos pokyčių, kol pokytis neatitinka informacinių sistemų modernizavimo kriterijų, priima informacinės sistemos duomenų valdymo įgaliotinis;

22.5. informacinės sistemos modernizavimą ir likvidavimą inicijuoja duomenų valdymo įgaliotinis;

22.6. sprendimus dėl informacinės sistemos modernizavimo ir likvidavimo priima informacinės sistemos valdytojo vadovas;

22.7. sprendimus dėl informacinės sistemos saugos būsenai užtikrinti būtinų informacinės sistemos pokyčių priima informacinės sistemos saugos įgaliotinis;

22.8. sprendimus dėl informacinės sistemos infrastruktūros funkcionavimui užtikrinti būtinų saugos pataisų įgyvendinimo inicijuoja ir informavęs atsakingus asmenis diegia informacinės sistemos infrastruktūrą prižiūrintis administratorius;

22.9. visi potencialūs pokyčiai registruojami elektroniniame informacinės sistemos pokyčių registre;

22.10. informacinės sistemos funkcijų ir galimybių sąrankos aprašai turi būti atnaujinami ir atspindėti esamą informacinės sistemos sąrankos būklę;

22.11. taikomosios programinės įrangos pokyčiai įgyvendinami duomenų valdymo įgaliotinio patvirtintu eiliškumu;

22.12. prieš atlikdamas informacinės sistemos pokyčius, kurių metu gali iškilti grėsmė duomenų ir informacinės sistemos konfidencialumui, vientisumui ar pasiekiamumui, informacinės sistemos administratorius organizuoja informacinės sistemos pokyčių testavimą bandomojoje aplinkoje;

22.13. atlikęs vykdomų informacinės sistemos pokyčių testavimą, informacinės sistemos administratorius gali pradėti įgyvendinti informacinės sistemos pokyčius tik:

22.13.1. gavęs patvirtinimą ir suderinęs pokyčio diegimo grafiką su atsakingais asmenimis (duomenų valdymo įgaliotinis, informacinės sistemos saugos įgaliotinis, Universiteto Informacinių technologijų pagalbos centro Informacinių technologijų pagalbos skyrius);

22.13.2. ne vėliau kaip prieš 2 (dvi) darbo dienas iki informacinės sistemos pokyčių vykdymo pradžios elektroniniu paštu informavęs atsakingus asmenis ir elektroniniu būdu sistemoje informavęs naudotojus apie tokių darbų pradžią ir galimus informacinės sistemos veikimo sutrikimus.

23. Naudotojų funkcijoms ir informacinės sistemos administratorių pareigoms atlikti gali būti naudojami nešiojami kompiuteriai ir mobilieji įrenginiai, kuriems taikomi šie papildomi reikalavimai:

23.1. Išvežti iš patalpų nešiojamieji kompiuteriai ir mobilieji įrenginiai negali būti palikti be priežiūros viešose vietose.

23.2. Įrenginiai turi būti rakinami slaptažodžiais pagal informacinės sistemos naudotojui nustatytą autentifikavimo reikalavimų lygį.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINĖS SISTEMOS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

24. Reikalavimai paslaugų teikėjų teikiamoms paslaugoms nustatomi šių paslaugų teikimo sutartyse.

25. Paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja informacinės sistemos taikomąją programinę įrangą, naudodamas:

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

25.2. informacinės sistemos testinės duomenų bazės duomenis (informacinės sistemos taikomajai programinei įrangai modifikuoti);

25.3. tik legalią sisteminę programinę įrangą.

26. Paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos:

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

26.2. informacinės sistemos administratorius, suteikdamas prieigos prie informacinės sistemos duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie informacinės sistemos duomenų sąlygomis;

26.3. pasibaigus sutartyje nurodytam laikotarpiui, informacinės sistemos administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie informacinės sistemos duomenų teisę.

27. informacinės sistemos administratoriai ir naudotojai, pažeidę šių taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____