PATVIRTINTA
Vilniaus universiteto rektoriaus
2018 m. gegužės 3 d. įsakymu Nr. R-271

ANGLŲ-LIETUVIŲ-ANGLŲ IR PRANCŪZŲ-LIETUVIŲ-PRANZŪZŲ KALBŲ MAŠININIO VERTIMO, PAREMTO STATISTINIAIS METODAIS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Anglų – lietuvių - anglų ir prancūzų – lietuvių – prancūzų kalbų mašininio vertimo, paremto statistiniais metodais informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato Anglų – lietuvių - anglų ir prancūzų – lietuvių – prancūzų kalbų mašininio vertimo, paremto statistiniais metodais, informacinės sistemos (toliau – informacinė sistema) valdytojo, tvarkytojo, jo paskirtų informacinės sistemos administratorių, informacinės sistemos saugos įgaliotinio ir informacinės sistemos naudotojų atsakomybę ir veiksmus, užtikrinančius saugų informacinės sistemos techninės ir programinės įrangos funkcionavimą, informacinės sistemos duomenų tvarkymą ir teikimą informacinės sistemos duomenų gavėjams.

2. Taisyklės parengtos vadovaujantis 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“ (toliau - Techniniai reikalavimai), 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) reikalavimais, Anglų – lietuvių - anglų ir prancūzų – lietuvių – prancūzų kalbų mašininio vertimo, paremto statistiniais metodais, informacinės sistemos nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2012 m. spalio 29 d. įsakymu R-401 „Dėl Anglų – lietuvių - anglų ir prancūzų – lietuvių – prancūzų kalbų mašininio vertimo, paremto statistiniais metodais, informacinės sistemos ALPMAVIS nuostatų tvirtinimo“ (toliau – informacinės sistemos nuostatai), informacinės sistemos duomenų saugos nuostatais, 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. Visi registruoti informacinės sistemos naudotojai ir administratoriai susipažįsta ir sutinka su šiomis taisyklėmis pasirašytinai arba elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

5. Taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“, Techniniuose reikalavimuose, Informacinės sistemos nuostatuose, informacinės sistemos duomenų saugos nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

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

6.1. Informacinės sistemos administratorių (toliau - administratoriai) tvarkoma informacija;

6.2. registruotų informacinės sistemos naudotojų tvarkoma informacija;

6.3. kitų informacinės sistemos naudotojų tvarkoma informacija.

7. Visi informacinės sistemos naudotojai:

7.1. gali vykdyti paieškas, peržiūrėti informaciją, nurodytą Informacinės sistemos nuostatų 15 punkte.

8. Registruoti naudotojai:

8.1. gali vykdyti paieškas ir peržiūrėti informaciją, nurodytą Informacinės sistemos nuostatų 15 punkte;

8.2. gali pateikti atsiliepimus;

8.3. užsiprenumeruoti naujienas;

8.4. kurti ir peržiūrėti komentarus diskusijų forume;

8.5. kurti ir keisti savo profilio duomenis;

8.6. kurti ir keisti savo pateiktus žodynus:

9. Informacinės sistemos administratorius atsakingas už šios informacijos tvarkymą:

9.1. naudotojų duomenys;

9.2. naudotojų vaidmenys;

9.3. naudotojų teisės;

9.4. bendras sistemos turinys;

9.5. duomenų bazių duomenys.

9.6. paslaugų iniciavimo ir teikimo duomenys;

9.7. paslaugų teikimą aprašantys duomenys;

9.8. paslaugų teikimo stebėsenos duomenys:

9.8.1. duomenų užklausimo laikas;

9.8.2. duomenų perdavimo laikas;

9.8.3. paslaugų suteikimo laikas;

9.8.4. kiti techniniai duomenys paslaugų teikimo stebėsenai atlikti.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

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

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

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

11. Kompiuterinės įrangos saugos priemonės:

11.1. prieigos prie informacinės sistemos tarnybinių stočių (serverių) kontrolė užtikrinama suteikiant prieigos teises tik administratoriams;

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

11.3. kompiuterinės įrangos gedimų registravimas kompiuterinės įrangos gedimų žurnale;

11.4. informacinės sistemos administratorių kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti darbo vietos administratorių apie tai, kuriems kompiuteriams yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

11.5. turi būti operatyviai ištestuojami ir įdiegiami kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

11.6. 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;

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

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

12. Sisteminės ir taikomosios programinės įrangos saugos priemonės informacinės sistemos tvarkytojo darbo stotyse ir darbuotojų kompiuterinėje įrangoje:

12.1. turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

12.2. programinės įrangos diegimą atlieka tik įgalioti asmenys;

12.3. naudojamos darbo stotyse autorizuotos programinės įrangos sąrašą rengia ir atnaujina informacinės sistemos administratorius;

12.4. neatliekant jokių veiksmų su informacine sistema 30 minučių, turi būti užtikrinta, kad toliau naudotis informacine sistema galima būtų tik pakartotinai patvirtinus savo tapatybę;

12.5. 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;

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

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

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

13. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

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

13.2. 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;

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

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

14.1. informacinės sistemos tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

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

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

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

14.5. įvykus sistemos gedimui, pildomas įėjimo punkto žurnalas, nurodant pateikimo priežastį, pradžią ir pabaigą;

14.6. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

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

14.8. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

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

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

15.3. supažindinimas informacinės sistemos sistemoje įgyvendinamas užtikrinant susipažinimo įrodomumą;

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

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

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

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

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

15.9. 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;

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

15.11. 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;

15.12. informacinės sistemos asmens duomenų saugumas užtikrinamas vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms.

16. Informacinės sistemos naudotojų veiksmų registravimo tvarka:

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

16.2. 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.

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

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

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

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

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

17.1. už informacinės sistemos elektroninės informacijos atsarginių kopijų darymą yra atsakingas administratorius;

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

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

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

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

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

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

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

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

17.10. už visiškus informacinės sistemos atkūrimo bandymus atsako administratorius. Elektroninės informacijos atkūrimo bandymų metodai nustatomi veiklos tęstinumo plane.

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

18.1. informacinės sistemos elektroninė informacija yra teikiama institucijoms, kitiems juridiniams ir fiziniams asmenims (toliau – duomenų gavėjai), kai Lietuvos Respublikos įstatymai ir (ar) Europos Sąjungos teisės aktai nenustato kitaip;

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

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

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

18.5. 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;

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

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

18.8. 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.

18.9. už informacinės sistemos elektroninės informacijos perkėlimą iš susijusių informacinių sistemų bei, poreikiui esant, elektroninės informacijos teikimas kitoms informacinėms sistemoms yra atsakingas duomenų valdymo įgaliotinio paskirtas informacinės sistemos administratorius;

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

19.1. 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;

19.2. informacinės sistemos naudotojas, įtaręs, kad su informacinės sistemos duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai savo darbo vietos administratoriui;

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

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

19.5. 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.

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

20.1. informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka su trečia 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.

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

21.1. 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;

21.2. 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;

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

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

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

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

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

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

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

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

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

21.12. 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;

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

21.13.1. gavęs patvirtinimą ir suderinęs pokyčio diegimo grafiką su atsakingais asmenimis (duomenų valdymo įgaliotinis, saugos įgaliotinis, naudotojų aptarnavimo skyrius);

21.13.2. ne vėliau kaip prieš 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.

22. Informacinės sistemos naudotojų funkcijoms ir administratorių pareigoms atlikti gali būti naudojami nešiojami kompiuteriai ir mobilieji įrenginiai, kuriems taikomi šie papildomi reikalavimai:

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

22.2. 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

23. Sudarius informacinės sistemos funkcionavimui reikalingų paslaugų teikimo sutartį su paslaugų teikėju, paslaugų teikimo sutartyse turi būti nurodoma, kad:

23.1. paslaugų teikėjas kuria ar modifikuoja informacinės sistemos taikomąją programinę įrangą, naudodamas įgyvendintas elektroninės informacijos saugos nuo nesankcionuoto poveikio sisteminei, programinei įrangai ir patalpoms priemones, kurios privalo atitikti informacinės sistemos duomenų saugos nuostatų bei kitų informacinės sistemos saugos politiką įgyvendinančių teisės aktų reikalavimus;

23.2. pokyčius diegti leidžiama tik ištestavus juos informacinės sistemos tvarkytojo tam skirtoje aplinkoje;

23.3. pokyčiai į gamybinę aplinką diegiami tik iš anksto informavus informacinės sistemos naudotojus ir administratorius, sutartu techninės profilaktikos laiku.

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

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

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

24.3. pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui, informacinės sistemos administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie informacinės sistemos duomenų teisę ir apie tai jį informuoja.

25. Informacinės sistemos administratoriai ir naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.