PATVIRTINTA
Vilniaus universiteto rektoriaus
2016 m. vasario 2 d. įsakymu Nr. R-63

LIETUVIŲ ŠNEKA VALDOMŲ PASLAUGŲ INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Lietuvių šneka valdomų paslaugų informacinės sistemos (toliau – informacinė sistema) saugaus elektroninės informacijos tvarkymo taisyklių tikslas – nustatyti informacinės sistemos 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 teikėjams.

2. Informacinės sistemos saugaus elektroninės informacijos tvarkymo 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, 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, informacinės sistemos nuostatais, patvirtintais Vilniaus universiteto rektoriaus 2014 m. vasario 21 d. įsakymu R-87 (toliau – informacinės sistemos nuostatai), informacinės sistemos duomenų saugos nuostatais (toliau – informacinės sistemos saugos nuostatai), patvirtintais Vilniaus universiteto rektoriaus 2015 m. rugsėjo 28 d. įsakymu R-363, 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. Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse naudojamos sąvokos:

5.1. Išorinis informacinės sistemos naudotojas – nesusijęs sutartiniais santykiais su informacinės sistemos valdytoju arba tvarkytoju fizinis asmuo, turintis teisę peržiūrėti nuostatų III skyriaus 13.1 ir 13.2.1-13.2.6 punktuose išvardintą elektroninę informaciją;

5.2. Vidinis informacinės sistemos naudotojas – informacinės sistemos naudotojas, darbo santykiais susijęs su informacinės sistemos valdytoju arba informacinės sistemos tvarkytoju, tvarkantis visus nuostatų III skyriaus 13 punkte išvardintus duomenis;

5.3. Informacinės sistemos taikomosios arba sisteminės įrangos administratorius – vidinis informacinės sistemos naudotojas, prižiūrintis informacinę sistemą ir (ar) jos infrastuktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą, ar kitas asmuo (asmenų grupė), kuriam 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).

5.4. informacinės sistemos administratorius (toliau – administratorius) – informacinės sistemos tvarkytojo darbuotojas, dirbantis pagal darbo sutartį, kuriam tvarkytojas paskyrė pareigą ir teisę koordinuoti informacinės sistemos taikomosios ir sisteminės įrangos administratorių grupės ar paslaugų teikėjo darbą prižiūrint informacinę sistemą ir (ar) jos infrastuktūrą.

5.5. Kitos informacinės sistemos naudotojų administravimo taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, Saugos dokumentų turinio gairėse, informacinės sistemos nuostatuose, informacinės sistemos duomenų saugos nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

6. Informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių) sąrašas pateikiamas informacinės sistemos nuostatų III skyriaus 13 punkte.

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

7.1. administratorių tvarkoma informacija;

7.2. naudotojų tvarkoma informacija.

8. Išorinių neregistruotų naudotojų tvarkoma informacija:

8.1. gali vykdyti paieškas, peržiūrėti informaciją Nuostatų III skyriaus 13.2.1-13.2.6 punktuose;

8.2. gali pateikti atsiliepimus (Nuostatų III skyriaus 13.2.5 punktas);

9. Išorinių registruotų naudotojų tvarkoma informacija:

9.1. gali vykdyti paieškas ir peržiūrėti informaciją Nuostatų III skyriaus 13.2.1-13.2.6 punktuose;

9.2. gali pateikti atsiliepimus (Nuostatų III skyriaus 14.4.6 punktas);

9.3. užsiprenumeruoti naujienas (Nuostatų III skyrius 14.4.5 punktas);

9.4. kurti ir peržiūrėti komentarus diskusijų forume (Nuostatų III skyrius 14.4.9);

9.5. kurti ir keisti savo profilio duomenis (Nuostatų III skyriaus 13.1.2, 13.1.5 punktai);

10. Vidinių naudotojų tvarkoma informacija:

10.1. gali vykdyti paieškas, peržiūrėti ir keisti informaciją, nurodytą Nuostatų III skyriaus 13 punkte.

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

11.1. naudotojų duomenys;

11.2. naudotojų vaidmenys;

11.3. naudotojų teisės;

11.4. bendras sistemos turinys (bendras puslapių turinys, atsiliepimai, nuorodos, galerijos, video ir audio įrašai);

12. Sisteminis administratorius atsakingas už šios informacijos tvarkymą:

12.1. paslaugų iniciavimo ir teikimo duomenys;

12.2. paslaugų teikimą aprašantys duomenys;

12.3. paslaugų teikimo stebėsenos duomenys:

12.3.1. duomenų užklausimo laikas;

12.3.2. duomenų perdavimo laikas;

12.3.3. paslaugų suteikimo laikas;

12.3.4. kiti techniniai duomenys paslaugų teikimo stebėsenai atlikti.

13. Informacinės sistemos vidiniai naudotojai ir administratoriai atsakingi už informacinės sistemos nuostatų III skyriaus 13 punkte aprašytos informacijos tvarkymą.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

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

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

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

15. Kompiuterinės įrangos saugos priemonės:

15.1. 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;

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

15.3. kompiuterinės įrangos gedimų registravimas kompiuterinės įrangos gedimų žurnale;

15.4. 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;

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

15.6. informacinės sistemos sisteminiai 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;

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

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

16. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

16.1. informacinės sistemos tvarkytojo darbo stotyse ir darbuotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

16.2. programinės įrangos diegimą atlieka tik įgalioti asmenys;

16.3. naudojamos autorizuotos programinės įrangos sąrašą rengia ir reguliariai atnaujina tvarkytojo informacinės sistemos sisteminis administratorius;

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

16.5. 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;

16.6. turi būti operatyviai ištestuojami ir įdiegiami informacinės sistemos tarnybinių stočių įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; informacinės sistemos administratoriai 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;

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

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

17. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

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

17.2. 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;

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

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

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

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

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

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

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

18.6. įvykių žurnalas privalo būti pateiktas saugos įgaliotiniui pareikalavus;

18.7. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

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

18.9. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

19.1. informacinės sistemos duomenis keisti, atnaujinti ir įrašyti gali tik autorizuoti informacinės sistemos naudotojai turintys teisę tai atlikti;

19.2. informacinės sistemos duomenis teisėtai gali būti naikinami tik autorizuotų informacinės sistemos naudotojų, turinčių teisę tai atlikti;

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

19.4. supažindinimas informacinės sistemos sistemoje įgyvendinamas užtikrinant susipažinimo įrodomumą;

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

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

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

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

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

19.10. 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;

19.11. informacinės sistemos duomenys informacinės sistemos duomenų bazėje saugomi neterminuotai nuo paskutinio pakeitimo (papildymo);

19.12. informacinės sistemos esantys asmens duomenys informacinės sistemos duomenų bazėje saugomi 3 (tris) metus nuo paskutinio pakeitimo (papildymo). Pasibaigus saugojimo terminui arba informacinės sistemos naudotojui panaikinus savo paskyrą informacinės sistemos sistemoje, informacinės sistemos naudotojo asmens duomenys ištrinami iš informacinės sistemos;

19.13. informacinės sistemos asmens duomenų saugumas užtikrinamas vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12).

20. Informacinės sistemos naudotojų veiksmų registravimo tvarka:

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

20.2. 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.

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

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

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

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

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

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

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

21.3. informacinės sistemos duomenų bazių ir archyvų valdymas organizuojamas atsižvelgiant į informacinės sistemos nuostatų 42 punkto reikalavimus;

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

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

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

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

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

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

21.10. visiški informacinės sistemos elektroninės informacijos atkūrimo bandymai vykdomi ne darbo valandomis ir prieš tai informavus visus informacinės sistemos naudotojus;

21.11. už visiškus informacinės sistemos atkūrimo bandymus yra atsakingas informacinės sistemos sisteminis administratorius. Elektroninės informacijos atkūrimo bandymų metodai nustatomi veiklos tęstinumo plane.

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

22.1. 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;

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

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

22.4. informacinės sistemos interneto svetainėje (portale) viešinami informacinės sistemos nuostatų 13.2 punkte nurodyti duomenys.

22.5. tretiesiems asmenims, turintiems teisę pagal Lietuvos Respublikos teisės aktus gauti sistemoje tvarkomus 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;

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

22.7. sistemos nuostatuose nurodytiems duomenų gavėjams duomenys teikiami neatlygintinai;

22.8. 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.

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

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

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

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

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

23.4. Sisteminis administratorius išanalizuoja gautą informaciją, įvertina, ar nereikėtų papildomų prevencinių priemonių;

23.5. apie pažeidimo faktą, atliktus veiksmus pažeidimo pasekmių likvidavimui ir jo pasikartojimo prevencijai bei siūlomas papildomas priemones sisteminis administratorius informuoja pagrindinio informacinės sistemos tvarkytojo administratorių ir saugos įgaliotinį;

23.6. 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.

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

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

24.2. informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka 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), aprašoma paslaugų, susijusių su informacinės sistemos programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

25. informacinės sistemos pokyčių valdymo tvarka:

25.1. 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 ir skubumas) pokyčių prioritetų nustatymo (eiliškumas) procesus;

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

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

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

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

25.6. informacinės sistemos funkcijų ir galimybių sąrankos aprašai turi būti atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę;

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

25.8. visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su informacinės sistemos duomenų valdymo įgaliotiniu ir vykdomi tik gavus raštišką pritarimą;

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

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

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

25.12. planuodamas informacinės sistemos pokyčius, kurių metu galimi informacinės sistemos veikimo sutrikimai, informacinės sistemos sisteminis administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki informacinės sistemos pokyčių vykdymo pradžios elektroniniu paštu informuoti informacinės sistemos administratorius ir elektroniniu būdu sistemoje informuoti naudotojus apie tokių darbų pradžią ir galimus informacinės sistemos veikimo sutrikimus.

26. Tvarkytojo vidinių naudotojų pareigoms atlikti naudojamų nešiojamų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

26.1. vidinių 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 informacinės sistemos administratorių kompiuteriai turi būti saugomi ir rakinami fizinei apsaugai skirtomis grandinėmis;

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

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

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

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

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

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

28.3. tik legalią sisteminę programinę įrangą.

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

29.1. 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 sisteminis administratorius suteikia fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti;

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

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

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

SUDERINTA
Lietuvos Respublikos
vidaus reikalų ministerijos
2016-01-28 raštu Nr. 1D-555