VILNIAUS UNIVERSITETO
REKTORIAUS

ĮSAKYMAS
DĖL LIETUVIŲ ŠNEKA VALDOMŲ PASLAUGŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ TVIRTINIMO IR ATSAKINGŲ ASMENŲ SKYRIMO

2015 m. rugsėjo 28 d. Nr. R-363
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 8 ir 12 punktais, bei Vilniaus universiteto Statuto 43 straipsnio 1 dalies 19 punktu:

1. T v i r t i n u Lietuvių šneka valdomų paslaugų informacinės sistemos (toliau - LIEPA) duomenų saugos nuostatus.
2. S k i r i u Vilniaus universiteto Matematikos ir informatikos instituto direktorių prof. Gintautą Dzemydą informacinės sistemos LIEPA duomenų valdymo įgaliotiniu.
3. Į g a l i o j u Vilniaus universiteto Matematikos ir informatikos instituto direktorių prof. Gintautą Dzemydą per 1 mėnesį po duomenų saugos nuostatų patvirtinimo paskirti informacinės sistemos LIEPA administratorius.
4. P a v e d u Informacinės sistemos LIEPA duomenų saugos įgaliotiniui Gediminui Navickui per 1 mėnesį parengti šiuos informacinės sistemos LIEPA saugos dokumentus:
   4.1. Saugaus elektroninės informacijos tvarkymo taisykles;
   4.2. Naudotojų administravimo taisykles.
5. N u s t a t a u , kad informacinei sistemai LIEPA bus taikomas Vilniaus universiteto Informacinių technologijų taikymo centro teikiamų paslaugų ir tvarkomų informacinių sistemų veiklos tęstinumo valdymo planas.

Rektorius prof. Artūras Žukauskas

Parengė: ITTC saugos įgaliotinis Viktoras Bulavas, tel. 236 6202

PROJEKTAS

PATVIRTINTA
Vilniaus universiteto
rektoriaus 2015-09-28
<data> įsakymu Nr. <numeris>
R-363

LIETUVIŲ ŠNEKA VALDOMŲ PASLAUGŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvių šneka valdomų paslaugų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvių šneka valdomų paslaugų informacinės sistemos (toliau – informacinė sistema) elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir informacinės sistemos naudotojų supažindinimo su saugos dokumentais principus.

2. Informacinės sistemos Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos informaciją, užtikrinti elektroninės informacijos prieinamumą ir vientisumą.

3. Saugos nuostatuose vartojamos sąvokos atitinka Saugos nuostatų 11 straipsnyje nurodytuose teisės aktuose vartojamas sąvokas.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos prieinamumo užtikrinimas;

4.2. elektroninės informacijos vientisumo užtikrinimas;

4.3. informacinės sistemos veiklos tęstinumas.

5. Informacinės sistemos valdytojas ir tvarkytojas yra Vilniaus universitetas, Universiteto g. 3, LT-01513, Vilnius. Informacinės sistemos valdytojo funkcijas atlieka Vilniaus universiteto Matematikos ir informatikos institutas. Informacinės sistemos tvarkytojo funkcijas atlieka Vilniaus universiteto Informacinių technologijų taikymo centras.

6. Informacinės sistemos valdytojo teisės ir pareigos:

6.1. Metodiškai vadovauja informacinės sistemos tvarkytojui ir koordinuoja informacinės sistemos funkcionavimą.

6.2. Informacinės sistemos valdytojas turi teisę:

6.2.1. rengti ir priimti teisės aktus, susijusius su duomenų tvarkymu ir duomenų sauga;

6.2.2. spręsti informacinės sistemos plėtros klausimus;

6.2.3. perduoti Valstybės informacinių išteklių įstatymo 41 straipsnyje numatytu būdu paskirtam paslaugos teikėjui atlikti informacinės sistemos techninės ir programinės įrangos priežiūrą ir (arba) informacijos tvarkymo funkcijas, išskyrus funkcijas, susijusias su sprendimų dėl informacijos teikimo ir skelbimo, ir su asmenų, tvarkančių informaciją, teisių ir pareigų nustatymo priėmimu.

6.2.4. kitas informacinės sistemos nuostatuose ir kituose teisės aktuose nustatytas teises.

6.3. Informacinės sistemos valdytojas privalo:

6.3.1. koordinuoti informacinės sistemos tvarkytojo ir šio įstatymo 41 straipsnyje numatyto teikėjo darbą, nustatyta tvarka atlikti jų priežiūrą;

6.3.2. atlikti duomenų saugos reikalavimų laikymosi priežiūrą;

6.3.3. nagrinėti informacinės sistemos tvarkytojo pasiūlymus dėl informacinės sistemos veiklos tobulinimo ir priimti dėl jų sprendimus;

6.3.4. užtikrinti, kad informacinė sistema būtų tvarkoma vadovaujantis įstatymu, informacinės sistemos nuostatais ir kitais teisės aktais;

6.3.5. atlikti kitus informacinės sistemos nuostatuose ir kituose teisės aktuose nustatytus veiksmus.

7. Informacinės sistemos tvarkytojas tvarko duomenis ir atsako už jų saugą.

7.1. Informacinės sistemos tvarkytojas privalo:

7.1.1. užtikrinti, kad valstybės informacinė sistema veiktų nepertraukiamai;

7.1.2. užtikrinti nepertraukiamą informacinės sistemos veikimą, elektroninės informacijos, esančios informacinėje sistemoje, saugą ir saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

7.1.3. užtikrinti tinkamą informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

7.2. Informacinės sistemos tvarkytojas turi teisę:

7.2.1. teikti pasiūlymus, kaip tobulinti informacinės sistemos saugą;

7.2.2. kitas informacinės sistemos nuostatuose ir kituose teisės aktuose nustatytas teises.

7.3. Informacinės sistemos tvarkytojo vadovas yra atsakingas už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politikos įgyvendinamuosiuose dokumentuose nustatyta tvarka.

8. Informacinės sistemos duomenų valdymo įgaliotinis, vadovaudamasis informacinių technologijų plėtros planu, kitais institucijos planavimo dokumentais:

8.1. įgyvendina informacinės sistemos plėtrą;

8.2. tiesiogiai prižiūri, kaip kuriama ir tvarkoma informacinė sistema, diegiama programinė įranga, panaudojamos investicijos;

8.3. rengia informacinės sistemos biudžetų projektus;

8.4. tiesiogiai prižiūri, kad informacija, duomenys, dokumentai ir (arba) jų kopijos būtų teikiami, skelbiami ir (arba) perduodami pagal teisės aktuose nustatytus reikalavimus;

8.5. teikia pasiūlymus dėl darbuotojų, kuriems pavesta tvarkyti informacinės sistemos duomenis, informaciją, dokumentus ir (arba) jų kopijas, teisių ir pareigų;

8.6. atlieka kitas teisės aktuose nustatytas funkcijas.

9. Informacinės sistemos saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

9.1.1. informacinės sistemos administratoriaus (administratorių) paskyrimo;

9.1.2. informacinių technologijų saugos atitikties vertinimo;

9.1.3. saugos dokumentų priėmimo, keitimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupė;

9.3. teikia informacinės sistemos administratoriui (administratoriams) privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo;

9.4. organizuoja informacinės sistemos rizikos įvertinimą;

9.5. periodiškai organizuoja informacinės sistemos administratorių mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas;

9.6. atlieka kitas informacinės sistemos valdytojo ir/ar tvarkytojo vadovo pavestas ir kituose teisės aktuose jam priskirtas funkcijas;

9.7. informacinės sistemos saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą, yra atsakingas už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.

10. Informacinės sistemos administratorius (administratorių) funkcijos:

10.1. administruoja informacinės sistemos naudotojų duomenis;

10.2. analizuoja informacinės sistemos naudotojų veiksmų registracijos žurnalų įrašus;

10.3. kuria ir atkuria atsargines informacinės sistemos duomenų bazės kopijas;

10.4. rengia ir tikrina informacinės sistemos sąranką;

10.5. nustato pažeidžiamas informacinės sistemos vietas;

10.6. atlieka informacinės sistemos naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

10.7. įvertina informacinės sistemos naudotojų pasirengimą dirbti su informacine sistema;

10.8. informuoja informacinės sistemos saugos įgaliotinį apie saugos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

10.9. vykdo privalomus informacinės sistemos duomenų valdymo ir saugos įgaliotinio nurodymus;

10.10. prižiūrėdamas informacinės sistemą atsako už tinkama Saugos nuostatuose nustatytų funkcijų vykdymą.

11. Saugų informacinės sistemos duomenų tvarkymą reglamentuoja:

11.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

11.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

11.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);

11.4. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas 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“ (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas);

11.5. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

11.6. Lietuvos standartai LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

11.7. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2015 m. kovo 20 d. įsakymu Nr. 1T-13(1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014

m. gruodžio 18 d. įsakymo Nr. 1T-74 (1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymo Nr. 1T-12 (1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ pakeitimo“ pakeitimo“;

11.8. Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.9. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką (toliau – saugos politika) ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą bei duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. Informacinėje sistemoje tvarkoma elektroninė informacija priskirtina kitos elektroninės informacijos kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.4 papunkčio nuostatomis.

13. Informacinė sistema priskiriama ketvirtai kategorijai, vadovaujantis Valstybės informacinių išteklių įstatymo 3 straipsnio 4 dalimi, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.4 papunkčio nuostatomis, atsižvelgiant į joje apdorojamos elektroninės informacijos svarbos kategoriją.

14. Informacinėje sistemoje asmens duomenys tvarkomi tik vidaus administravimo reikmėms neautomatiniu būdu susistemintose rinkmenose, naudojant tik viešai skelbiamus asmens duomenis naudotojų paskyroms administruoti, todėl vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, priskiriamas pirmas tvarkomų asmens duomenų saugumo lygis.

15. Informacinės sistemos saugos įgaliotinis, vadovaudamasis Vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja informacinės sistemos rizikos veiksnių vertinimą. Prireikus, informacinės sistemos saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos veiksnių vertinimą.

16. Informacinės sistemos rizikos vertinimas surašomas rizikos įvertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo ir tvarkytojo vadovams.

17. Informacinės sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir

pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

17.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

17.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

18. Informacinės sistemos rizikos veiksniai vertinami priskiriant jų įtakos informacinės sistemos elektroninės informacijos saugai laipsnius, kurie nustatomi vadovaujantis šiais kriterijais:

18.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – informacija išsiųsta kitam adresatui, įvesti netikslūs duomenys, dingo dalis informacijos, kurią galima greitai atstatyti iš turimų atsarginių kopijų, prarasta informacija po paskutinio kopijavimo. Neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema kompiuterinėse darbo vietose;

18.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys netikslūs ar sugadinti, bet juos įmanoma atkurti iš turimų atsarginių kopijų. Duomenų bazių įrašai pakeisti, sunku rasti klaidas ir suklastotą informaciją, neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema tarnybinėse stotyse;

18.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys visiškai sugadinti, dėl vagystės, gaisro ar užliejimo prarasti ne tik duomenys iš duomenų bazių, bet ir atsarginės kopijos, neveikia visa informacinė sistema.

19. Informacinės sistemos rizikos vertinimo metu atliekami darbai:

19.1. informacinę sistemą sudarančių vertybių nustatymas ir įvertinimas;

19.2. rizikos veiksnių įtakos informacinės sistemos veiklai vertinimas;

19.3. saugos priemonių nustatymas.

20. Informacinės sistemos valdytojas, atsižvelgdamas į informacinės sistemos rizikos įvertinimo ataskaitą, prireikus tvirtina informacinės sistemos rizikos įvertinimo ir rizikos

valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis informacinės sistemos rizikos valdymo priemonėms įgyvendinti.

21. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

21.1. liekamoji rizika turi būti sumažinama iki priimtino lygio;

21.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

21.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

22. Atlikus rizikos įvertinimą, esant poreikiui, informacinės sistemos saugos įgaliotinis rengia ir teikia valdytojui tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

23. Siekiant užtikrinti informacinės sistemoms Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, informacinės sistemos saugos įgaliotinis, ne rečiau kaip kartą per du metus, vadovaujantis Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ patvirtinta metodika, atlikus rizikos vertinimą organizuoja informacinės sistemos saugos atitikties vertinimą, kurio metu:

23.1. surenkama vertinimui būtina informacija apie informacinių technologijų saugos padėtį Vilniaus universiteto informacinėse sistemose ir dokumentai, būtini užtikrinant informacinės sistemos saugą;

23.2. įvertinama Saugos nuostatų ir saugos politiką įgyvendinančių teisės aktų atitiktis Bendriesiems duomenų saugumo reikalavimams. Vertinimo metu vertintojas gali atlikti informacinės sistemos naudotojų ir administratorių apklausą;

23.3. vertintojas parengia informacinių sistemų saugos atitikties vertinimo ataskaitą ir teikia ją atitinkamam vadovui, kuris organizuoja trūkumų šalinimo priemonių plano rengimą.

24. Atlikus informacinės sistemos saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato valdytojo vadovas.

25. Trūkumų šalinimo priemonių plano vykdymo kontrolę užtikrina informacinės sistemos saugos įgaliotinis.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Programinės įrangos, skirtos informacinei sistemai nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

26.1. tarnybinėse stotyse ir kompiuterinėse darbo vietose privalo būti įdiegta apsauga nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.);

26.2. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per savaitę;

27. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

27.1. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

27.2. naudojama tik legali programinė įranga;

27.3. programinė įranga yra nuolatos atnaujinama laikantis gamintojo reikalavimų;

27.4. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik informacinės sistemos administratoriai.

28. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. proxy) ir kt.) pagrindinės naudojimo nuostatos:

28.1. įmonės kompiuteriniai tinklai nuo viešųjų telekomunikacijų tinklų (interneto) atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

28.2. visas informacinės sistemos duomenų srautas į ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenkėjiškos programinės įrangos;

28.3. Papildomos priemonės kompiuteriams ir mobiliems įrenginiams, kurie gali būti panaudoti nustatytoms administravimo funkcijoms atlikti ne institucijos patalpose, nustatomos Saugaus elektroninės informacijos tvarkymo taisyklėse.

29. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

29.1. nuotolinis prisijungimas prie informacinės sistemos galimas naudojantis „IPSec“ (angl. Internet Protocol Security) protokolų rinkiniu ir jungiantis kaip „IPSec“ programiniam klientui. Šia galimybe gali būti pasinaudota tik informacinės sistemos administravimo tikslais.

29.2. teikti elektroninę informaciją automatiniu būdu galima tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

30. Informacinės veiklos tęstinumo užtikrinimui elektroninė informacija yra periodiškai kopijuojama į rezervinių kopijų laikmenas kas 24 valandos ir laikmenos saugomos taip, kad avarijos atveju informacinę sistemą galima būtų atkurti taip, kad informacinės sistemos neveikimo laikotarpis būtų neilgesnis nei 24 valandos. Šios atsarginės duomenų kopijos turi būti

saugomos kitose patalpose nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate.

31. Informacinės sistemos prieinamumas per metus turi būti užtikrintas ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis.

IV. REIKALAVIMAI PERSONALUI

32. Informacinės sistemos saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais. Informacinės sistemos saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. Informacinės sistemos saugos įgaliotinis privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

33. Informacinės sistemos saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumo srityje, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau nei vieni metai.

34. Informacinės sistemos administratoriumi gali būti skiriamas/įdarbinimas darbuotojas, dirbantis pagal darbo sutartį, išmanantis darbą su kompiuterių tinklais ir mokantis užtikrinti jų saugumą. Informacinės sistemos administratorius privalo mokėti administruoti ir prižiūrėti duomenų bazes, būti susipažinęs su Saugos nuostatais ir saugos politikos įgyvendinamaisiais teisės aktais.

35. Informacinės sistemos administratoriai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti informacinės sistemos duomenis teisingumo ministro tvirtinamų Elektroninio dokumentų archyvo informacinės sistemos nuostatų nustatyta tvarka, būti susipažinę su Saugos nuostatais ir saugos politikos įgyvendinimą reglamentuojančiais teisės aktais.

36. Informacinės sistemos naudotojai ir administratoriai, pažeidę Saugos nuostatų ar kitų saugos politikos įgyvendinamųjų teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

37. Ne rečiau kaip kartą per du metus, rengiami duomenų saugos mokymai, kuriuos planuoja ir organizuoja informacinės sistemos saugos įgaliotinis.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Už informacinės sistemos naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politikos įgyvendinamaisiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas informacinės sistemos saugos įgaliotinis.

39. Informacinės sistemos naudotojų supažindinimą su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą organizuoja informacinės sistemos saugos įgaliotinis.

40. Su duomenų Saugos nuostatais susipažįstama pasirašytinai arba elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

41. Saugos nuostatai ir kiti saugos politikos įgyvendinamieji teisės aktai skelbiami informacinės sistemos naudotojams pasiekiamoje interneto svetainėje.

42. Pakartotinai su saugos politiką reguliuojančiais teisės aktais informacinės sistemos naudotojai supažindinami tik iš esmės pasikeitus informacijos saugą reguliuojantiems teisės aktams. Informacija apie saugos politikos įgyvendinamųjų teisės aktų pakeitimus siunčiama elektroniniu būdu.
