PATVIRTINTA
Lietuvos Respublikos švietimo
ir mokslo ministro 2013 m. liepos 4
d. įsakymu Nr. V-629

LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTERIJOS IR JAI PAVALDŽIŲ INSTITUCIJŲ FINANSŲ VALDYMO IR APSKAITOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos švietimo ir mokslo ministerijos ir jai pavaldžių institucijų finansų valdymo ir apskaitos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato organizacines, technines, administracines Lietuvos Respublikos švietimo ir mokslo ministerijos ir jai pavaldžių institucijų Finansų valdymo ir apskaitos informacinės sistemos (toliau – IS FVA) duomenų saugos priemones, skirtas užtikrinti duomenų ir informacijos tikslumą ir apsaugoti juos nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat bet kokio neteisėto tvarkymo, taip pat užtikrinti šių priemonių laikymąsi.

2. Saugos nuostatai parengti vadovaujantis:

2.1. Lietuvos Respublikos informacinių išteklių valdymo įstatymu (Žin., 2011, Nr. 163-7739);

2.2. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891);

2.3. Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070);

2.4. Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

2.5. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160);

2.6. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855)

3. Saugos nuostatai privalomi IS FVA naudotojams, tvarkytojams, administratoriui ir IS FVA Saugos įgaliotiniui (toliau – Saugos įgaliotinis).

4. IS FVA duomenų saugos tikslai:

4.1. IS FVA duomenų vientisumo, tikslumo užtikrinimas;

4.2. IS FVA duomenų prieinamumo užtikrinimas;

4.3. IS FVA duomenų konfidencialumo užtikrinimas;

4.4. IS FVA veiklos tęstinumo užtikrinimas.

5. Saugos nuostatuose vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, Saugos dokumentų turinio gairėse, kituose teisės aktuose ir Lietuvos standartuose LST ISO/IEC 17799:2006 ir LST ISO/IEC 27001:2006.

6. IS FVA saugumo svarba ir esama saugos padėtis yra nustatoma periodinės rizikos veiksnių įvertinimo metu ir pateikiama Rizikos įvertinimo ataskaitoje.

7. Saugos politika vykdoma šiomis prioritetinėmis kryptimis:

7.1. įgyvendinant atliekamų veiksmų su IS FVA duomenimis automatinį stebėjimą ir įrašų kaupimą;

7.2. įgyvendinant prieigos teisių prie IS FVA duomenų suteikimą ir duomenų naudotojo tapatumo identifikavimą;

7.3. įgyvendinant IS FVA duomenų kopijavimą, archyve esančių duomenų saugą;

7.4. įgyvendinant IS FVA duomenų saugą nuo žalingos programinės įrangos poveikio;

7.5. įrengiant saugias IS FVA tvarkyti skirtas patalpas ir kompiuterizuotas darbo vietas jose;

7.6. įgyvendinant IS FVA duomenų naudotojų kvalifikacijos tobulinimo sistemą;

7.7. integralumą su ataskaitų rinkiniui parengti informaciją teikiančiomis viešojo sektoriaus subjektų informacinėmis sistemomis;

7.8. įgyvendinant IS FVA duomenų saugos priemones nuo nesankcionuoto poveikio IS FVA programinei, techninei įrangai ir (ar) IS FVA programinės įrangos modifikavimo.

8. IS FVA valdytojas yra Lietuvos Respublikos švietimo ir mokslo ministerija (toliau – ŠMM).

9. IS FVA tvarkytojai yra dviejų tipų: pagrindinis IS FVA tvarkytojas Švietimo informacinių technologijų centras (toliau – ITC), ir kiti tvarkytojai, nurodyti IS FVA nuostatuose.

10. IS FVA valdytojas:

10.1. paskiria Saugos įgaliotinį arba paveda ITC direktoriui paskirti Saugos įgaliotinį;

10.2. tvirtina Saugos nuostatus, Saugaus elektroninės informacijos tvarkymo taisykles (toliau – Tvarkymo taisyklės), Informacinės sistemos veiklos tęstinumo valdymo planą (toliau – Valdymo planas), Informacinės sistemos naudotojų administravimo taisykles (toliau – Administravimo taisyklės);

10.3. koordinuoja IS FVA saugos reikalavimų laikymąsi;

10.4. turi teisę tikrinti, kaip IS FVA tvarkytojai laikosi nustatytų duomenų tvarkymo, duomenų saugos, veiklos tęstinumo užtikrinimo, naudotojų administravimo reikalavimų;

10.5. atlieka kitas teisės aktuose numatytas funkcijas.

11. IS FVA tvarkytojo -ITC direktorius turi:

11.1. švietimo ir mokslo ministrui pavedus, paskirti Saugos įgaliotinį, prižiūrėti IS FVA saugos politiką reglamentuojančių teisės aktų parengimą ir įgyvendinimą;

11.2. pavesti Saugos įgaliotiniui organizuoti ir kontroliuoti saugos politiką reglamentuojančių teisės aktų įgyvendinimą ITC;

11.3. pavesti Saugos įgaliotiniui sudaryti reglamentuojančių saugą dokumentų ir/arba nuorodų į juos komplektą, paskelbti jį specializuotoje svetainėje http://www.fva.smm.lt ir supažindinti kitų tvarkytojų vadovus arba jų paskirtus asmenis pasirašytinai;

11.4. paskirti IS FVA administratorių, jam pavesti užtikrinti IS FVA tarnybinės stoties saugų funkcionavimą, administruoti IS FVA duomenų bazę Saugos nuostatų ir kitų saugos politiką reglamentuojančių teisės aktų nustatyta tvarka;

11.5. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose numatytas funkcijas.

12. Kiti IS FVA tvarkytojai:

12.1. laikytis IS FVA saugą reglamentuojančių teisės aktų;

12.2. užtikrinti tinkamą techninės įrangos, naudojamos dirbti su IS FVA techninę priežiūrą.

13. Duomenų saugą reglamentuojančių teisės aktų įgyvendinimą organizuoja Saugos įgaliotinis, kuris:

13.1. gali teikti siūlymus ŠMM ir ITC dėl saugos dokumentų priėmimo, keitimo, panaikinimo, informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

13.2. reguliariai analizuoja gautą iš IS FVA administratoriaus ir kitų šaltinių IS FVA saugai galinčią turėti įtakos informaciją, vertina rizikos veiksnių tikėtinumus ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

13.3. koordinuoja saugos incidentų, įvykusių informacinėje sistemoje, tyrimą (išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupės);

13.4. teikia administratoriui privalomus vykdyti nurodymus ir pavedimus;

13.5. sudaro ir atnaujina reglamentuojančiu saugą dokumentų komplektą, skelbia jį specializuotoje svetainėje http://www.fva.smm.lt ir supažindina kitų institucijų – tvarkytojų vadovus arba jų įsakymais paskirtus asmenis pasirašytinai;

13.6. atlieka kitas švietimo ir mokslo ministro arba ITC direktoriaus, jeigu jį paskyrė ITC direktorius, pavestas ir teisės aktais nustatytas funkcijas.

14. IS FVA administratorius atlieka funkcijas, susijusias su IS FVA naudotojų pasirengimo dirbti su ja įvertinimu, naudotojų teisėmis, IS FVA sudarančiais komponentais (kompiuteriais, serveriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, duomenų perdavimo tinklais), šių komponentų sąranka, IS FVA pažeidžiamų vietų nustatymu, saugumo reikalavimų atitiktimi teisės aktų reikalavimams, pagal Saugos įgaliotinio nurodymus svarbių saugai įvykių ir informacijos rinkimu, išsaugojimu, sisteminimu ir pateikimu Saugos įgaliotiniui.

15. IS FVA duomenų sauga užtikrinama vadovaujantis Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 (Žin., 2013, Nr. 23-1122), Saugos dokumentų turinio gairėmis, Lietuvos standartu LST ISO/IEC 17799:2006, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, Saugos nuostatais, Tvarkymo taisyklėmis, Valdymo planu, Administravimo taisyklėmis, kitais teisės aktais, reglamentuojančiais saugų IS FVA duomenų tvarkymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. IS FVA priskiriama antrajai informacinės sistemos kategorijai. Kategorija priskirta vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairėmis.

17. IS FVA duomenis sudaro:

17.1. bendrieji (nurodyti IS FVA nuostatuose);

17.2. technologiniai (IS FVA naudotojo) duomenys.

18. IS FVA duomenis IS FVA duomenų gavėjams teikia IS FVA tvarkytojai IS FVA nuostatų ir kitų teisės aktų nustatyta tvarka.

19. IS FVA duomenų aktualumas užtikrinamas IS FVA duomenų teikėjų teikiamais aktualiais duomenimis ir IS FVA posistemių integruota veikla. Duomenų teikimo būdai ir periodiškumas nustatomas ITC direktoriaus tvirtinamame tvarkos apraše.

20. Saugos įgaliotinis IS FVA saugos atitikties vertinimą atlieka ne rečiau kaip kartą per metus. Saugos įgaliotinis teisės aktų nustatyta tvarka atlikdamas IS FVA saugos atitikties vertinimą, turi:

20.1. įvertinti saugos dokumentų ir realios informacijos saugos situacijos atitiktį;

20.2. inventorizuoti IS FVA techninę ir programinę įrangą;

20.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų IS FVA naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtas programas ir jų sąranką;

20.4. patikrinti (įvertinti) IS FVA naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

20.5. įvertinti pasirengimą užtikrinti IS FVA veiklos tęstinumą įvykus saugos incidentui.

21. Saugos įgaliotinis atlikęs saugos atitikties vertinimą, parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato švietimo ir mokslo ministras.

22. IS FVA turi perspėti administratorių, kai pagrindinėje IS FVA kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

23. Viešaisiais telekomunikaciniais tinklais perduodamos IS FVA elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. virtual private network, VPN), skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones.

24. IS FVA turi būti registruojami ir nustatytą laiką saugomi duomenys apie IS FVA įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis IS FVA, kitus saugai svarbius įvykius, nurodant IS FVA naudotojo identifikatorių ir įvykio laiką; ši informacija turi būti reguliariai analizuojama.

25. Institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti IS FVA įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; Valdymo planas turi užtikrinti IS FVA veiklos atnaujinimą atsarginėse patalpose per tokį laikotarpį, kad nebūtų nusižengta institucijos įsipareigojimams, susijusiems su IS FVA veikla.

26. Kopijų darymas turi būti fiksuojamas žurnale. Kopijos turi būti saugomos užrakintoje nedegioje spintoje.

27. Elektroninė informacija kopijose turi būti užšifruota arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtam elektroninės informacijos atkūrimui.

28. Periodiškai turi būti atliekami elektroninės informacijos atkūrimo iš kopijų bandymai.

29. Atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje.

30. Slaptažodį turi sudaryti ne mažiau kaip 6 simboliai ir slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių. Slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius.

31. Slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija. Pirmojo prisijungimo prie informacinės sistemos metu iš IS FVA naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį. Draudžiama slaptažodžius atskleisti tretiesiems asmenims.

32. Saugos įgaliotinis turi:

32.1. vieną kartą per kalendorinius metus švietimo ir mokslo ministro pavedimu arba ITC direktoriaus pavedimu, jeigu jį paskyrė ITC direktorius, įvertinti rizikos veiksnių tikėtinumą IS FVA duomenims, techninei, programinei įrangai, registravimo dokumentams, patalpoms, išnagrinėti įrašus rizikos veiksnių tikėtinumo registravimo žurnale, parengti Rizikos įvertinimo ataskaitą. Rizikos įvertinimo ataskaitą tvirtina švietimo ir mokslo ministras, arba ITC direktorius, priklausomai nuo to, kas pavedė atlikti rizikos įvertinimą;

32.2. per 10 kalendorinių dienų, patvirtinus Rizikos įvertinimo ataskaitą, parengti Trūkumų šalinimo planą (toliau – Planas), Plane nurodyti rizikos veiksnius šalinančias priemones, priemonių vykdymo terminus, vykdytojus. Planą tvirtina ITC direktorius.

33. Svarbiausieji rizikos veiksniai, kurie gali pažeisti IS FVA duomenų saugą, yra:

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

33.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai ir kita);

33.3. nenugalima jėga (force majeure).

34. Saugos nuostatų 31 punkte nurodytais, o prireikus ir kitais atvejais, IS FVA saugos įgaliotinis gali organizuoti neeilinį IS FVA rizikos veiksnių įvertinimą.

35. Neeilinis IS FVA rizikos veiksnių įvertinimas organizuojamas, kai:

35.1. įvyksta esminiai pokyčiai IS FVA techninėje ar programinėje įrangoje;

35.2. paaiškėja naujos tendencijos informacinių technologijų saugos srityje;

35.3. įvyksta IS FVA informacijos saugos incidentas.

36. Rizikos veiksnių IS FVA duomenims, techninei, programinei įrangai, registravimo dokumentams, patalpoms tikėtumui vertinti turi būti naudojama penkiabalė rizikos veiksnių tikėtinumo ir žalos vertinimo metodika:

36.1. nereikšmingas rizikos veiksnių tikėtinumas, žala – 1 balas;

36.2. mažas rizikos veiksnių tikėtinumas, žala – 2 balai;

36.3. vidutinis rizikos veiksnių tikėtinumas, žala – 3 balai;

36.4. didelis rizikos veiksnių tikėtinumas, žala – 4 balai;

36.5. labai didelis rizikos veiksnių tikėtinumas, žala – 5 balai.

37. Saugos priemonių parinkimo principai:

37.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

37.2. informacinės saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

37.3. esant galimybei turi būti įdiegtos prevencinės, korekcinės informacinės saugos priemonės.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

38. IS FVA duomenims apsaugoti nuo kenksmingos programinės įrangos turi būti naudojamos programines priemonės (viena iš jų): *Symantec Norton Antivirus, McAfee, Virus Scan, Panda AntiVirus, Kaspersky AntiVirus, Dr. Web* ir atnaujinamos ne rečiau kaip kartą per mėnesį.

39. IS FVA objektų duomenims saugiai rinkti, apdoroti, kaupti, saugoti, teikti švietimo ir mokslo registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims turi būti naudojamos programinės ir techninės įrangos naudojimą ribojančios priemonės, kuriose:

39.1. realizuota galimybė IS FVA duomenų naudotojams naudoti tik legalią programinę įrangą;

39.2. realizuota galimybė IS FVA duomenų naudotojams, jungiantis per https protokolą, taikyti prieigos prie IS FVA duomenų laiką;

39.3. realizuota IS FVA duomenų naudotojams prieigos prie IS FVA duomenų galimybė tik per registravimosi ir slaptažodžių sistemą;

39.4. realizuota galimybė IS FVA duomenų naudotojams ne rečiau kaip kartą per pusmetį atnaujinti slaptažodžius. Slaptažodžius draudžiama atskleisti tretiesiems asmenims;

39.5. naudojama IS FVA administravimo programinės įrangos ugniasienė;

39.6. realizuota galimybė nustatyti prieigos prie IS FVA duomenų autorius, fiksuoti jų atliktus veiksmus ir juos kaupti;

39.7. realizuota galimybė visas užklausas į IS FVA duomenų bazę fiksuoti programiniu būdu.

40. FVA IS techninės įrangos kontrolės priemonės:

40.1. vidinis tinklas nuo išorinio turi būti atskirtas papildoma užkarda;

40.2. tinklu gaunami duomenų srautai turi būti filtruojami;

40.3. siekiant identifikuoti FVA IS naudotojus ir jų veiksmus, naršymas FVA IS interneto svetainėje turi būti indeksuojamas ir saugomas vieną mėnesį;

40.4. visas gaunamas ir siunčiamas elektroninio pašto žinutes privalu tikrinti nuo virusų.

41. IS FVA duomenims tvarkyti paskirtuose darbuotojų kompiuteriuose:

41.1. draudžiama naudoti programinę ir techninę įrangą, nesusijusią su tiesiogine veikla ir funkcijomis, taip pat draudžiamas rinkmenų apsikeitimo programų naudojimas;

41.2. naudojama antivirusinė sistema nuo kenksmingos programinės įrangos poveikio atnaujinama ne rečiau kaip kartą per mėnesį;

41.3. prieiga, suteikianti galimybes tvarkyti FVA IS duomenis, suteikiama tik per registravimosi ir slaptažodžių sistemą.

42. ITC direktoriaus paskirtiems darbuotojams FVA IS tvarkyti draudžiama nešiojamuosius kompiuterius naudoti FVA IS duomenų perdavimui kompiuterių tinklais ne savo darbo vietoje.

43. FVA IS veiklos tęstinumui ir funkcionalumui užtikrinti duomenys periodiškai kopijuojami kas 12 valandų ir saugomi taip, kad įvykus avarijai veiklą iš atsarginių kopijų galima būtų atkurti per 24 valandas. Elektroninių bylų mėnesinės kopijos papildomai turi būti laikomos atskiroje patalpoje ir saugomos užrakintoje nedegioje spintoje.

44. FVA IS tarnybinėje stotyje neturi veikti programinė įranga, nesusijusi su FVA IS, švietimo ir mokslo registrų ir informacinių sistemų duomenų tvarkymu.

45. Saugos įgaliotinis turi organizuoti ITC IS FVA programinės, techninės įrangos naudojimą ribojančių priemonių įgyvendinimą.

46. IS FVA duomenų kopijų kūrimo tvarkos apraše, tvirtinamame ITC direktoriaus, turi būti nurodoma:

46.1. IS FVA duomenų kopijų kūrimo periodiškumas;

46.2. IS FVA duomenų kopijų saugojimo priemonės, būdai ir vieta;

46.3. IS FVA duomenų iš kopijų atkūrimo tvarka;

46.4. IS FVA duomenų kopijų naikinimo tvarka;

46.5. asmens, atsakingo už IS FVA duomenų kopijų kūrimą, saugojimą, atkūrimą, sunaikinimą, teisės ir pareigos.

IV. REIKALAVIMAI PERSONALUI

47. Saugos įgaliotinis privalo išmanyti pagrindinius informacijos saugos principus, turėti atitinkamą kvalifikaciją (kvalifikacijos tobulinimo kursai, pradinis saugaus darbo su duomenimis mokymas, ECDL vartotojo sertifikatas ar pan.), darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties, savo darbe vadovautis saugos politiką reglamentuojančiais teisės aktais.

48. IS FVA administratorius turi:

48.1. išmanyti darbą su kompiuterių tinklais;

48.2. turėti IS FVA tvarkyti naudojamų sisteminių programinių priemonių *Windows, Unix, Informix, Oracle, MS SQL* administravimo patirties;

48.3. mokėti administruoti informacinių sistemų duomenų bazes;

48.4. užtikrinti IS FVA saugą saugumo politiką reglamentuojančių teisės aktų nustatyta tvarka.

49. IS FVA duomenų naudotojai turi:

49.1. turėti darbo su kompiuteriu įgūdžių;

49.2. mokėti tvarkyti IS FVA duomenis IS FVA nuostatuose nurodyta tvarka;

49.3. išmanyti informacinių sistemų saugumo politiką reglamentuojančius teisės aktus.

50. Informacinių sistemų naudotojams gali būti rengiami informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., elektroniniu paštu, teminių seminarų

rengimas, atmintinės ir kt.). Saugos mokymus organizuoja ir jų veiksmingumą vertina Saugos įgaliotinis.

V. IS FVA NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

51. Saugos įgaliotinis organizuoja informacinių sistemų naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politiką reglamentuojančiais teisės aktais. Naudotojus supažindinant gali būti pateikiamos nuorodos į teisės aktus, esančius intraneto svetainėje ar vidiniame atitinkamai ŠMM arba ITC tinkle. Saugos įgaliotinis informuoja naudotojus apie Saugos nuostatų ar kitų saugos politiką reglamentuojančių teisės aktų pakeitimus.

VI. BAIGIAMOSIOS NUOSTATOS

52. Saugos nuostatai ir kiti saugos politiką reglamentuojantys teisės aktai turi būti peržiūrimi ne rečiau kaip kartą per metus. Saugos dokumentai turi būti peržiūrimi po rizikos analizės ar saugos atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami.

53. IS FVA tvarkytojai privalo įgyvendinti šiuose Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose IS FVA duomenų saugų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

54. Saugos įgaliotinis, IS FVA duomenų naudotojai, IS FVA administratorius raštu įsipareigoja nepažeisti šių Saugos nuostatų ir kitų teisės aktų, reglamentuojančių IS FVA duomenų saugų tvarkymą.

55. Duomenys apie IS FVA duomenų naudotojų, IS FVA administratoriaus atliktus veiksmus su IS FVA duomenimis saugomi Bendrųjų dokumentų saugojimo terminų rodyklėje nurodytais terminais, kurie taikomi IS FVA duomenims.

56. Saugos įgaliotinis, IS FVA duomenų naudotojai, IS FVA administratorius, pažeidę šių Saugos nuostatų, kitų teisės aktų, reglamentuojančių IS FVA duomenų saugų tvarkymą, reikalavimus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.