LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO
Į S A K Y M A S

DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2007 M. GRUODŽIO 22 D. ĮSAKYMO NR. V-1065 „DĖL SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINĖS SISTEMOS SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2012 m. balandžio 16 d. Nr. V-337
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2007 m. gruodžio 22 d. įsakymą Nr. V-1065 „Dėl Sveikatos apsaugos ministerijos informacinės sistemos saugos nuostatų patvirtinimo“ (Žin., 2008, Nr. 1-26):

1.1. Išdėstau antraštę taip:

„**DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ TVIRTINIMO**“.

1.2. Įrašau 1 punkte vietoj žodžių „saugos nuostatus“ žodžius „duomenų saugos nuostatus“.

1.3. Įrašau 2.1 punkte vietoj žodžių „Informacinių technologijų skyriaus vyriausiąjį specialistą Mantą Nausėdą“ žodžius „Bendrųjų reikalų departamento Informacinių technologijų skyriaus vyriausiąją specialistę Palmirą Ožalinskienę“.

1.4. Įrašau 2.2 punkte vietoj žodžių „Informacinių technologijų skyriaus vyresnįjį specialistą Mantą Vaičiulį Sveikatos apsaugos ministerijos informacinės sistemos administratoriumi“ žodžius „Bendrųjų reikalų departamento Informacinių technologijų skyriaus vyriausiąjį specialistą Jaroslavą Viduto Sveikatos apsaugos ministerijos informacinės sistemos administratoriumi ir Bendrųjų reikalų departamento Informacinių technologijų skyriaus vyriausiąjį specialistą Edgarą Tallat-Kelpšą Sveikatos apsaugos ministerijos informacinės sistemos administratoriumi“.

1.5. Išdėstau 3 punktą taip:

„3. P a v e d u Bendrųjų reikalų departamento Informacinių technologijų skyriui per 2 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir pateikti Lietuvos Respublikos sveikatos apsaugos ministrui tvirtinti Sveikatos apsaugos ministerijos informacinės sistemos veiklos tęstinumo valdymo planą, Sveikatos apsaugos ministerijos informacinės sistemos naudotojų administravimo taisykles“.

1.6. Išdėstau nauja redakcija nurodytuoju įsakymu patvirtintus Sveikatos apsaugos ministerijos informacinės sistemos saugos nuostatus (pridedama).

SVEIKATOS APSAUGOS MINISTRAS RAIMONDAS ŠUKYS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2012-03-22 raštu Nr. 1D-2060(52)

PATVIRTINTA
Lietuvos Respublikos
sveikatos apsaugos ministro
2007 m. gruodžio 22 d. įsakymu Nr. V-1065
(Lietuvos Respublikos
sveikatos apsaugos ministro
2012 m. balandžio 16 d. įsakymo Nr. V-337
redakcija)

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos sveikatos apsaugos ministerijos informacinės sistemos duomenų saugos nuostatai (toliau – nuostatai) nustato pagrindinius informacijos saugos užtikrinimo ir valdymo principus ir taisykles, kuriais vadovaujantis turi būti derinami informacinės sistemos veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys teisės aktai bei kiti dokumentai.

2. Nuostatai parengti vadovaujantis Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070) (toliau – Gairės). Nuostatuose vartojamos sąvokos atitinka Gairėse ir Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, patvirtintuose Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891) (toliau – Saugos reikalavimai), apibrėžtas sąvokas.

3. Sveikatos apsaugos ministerijos informacinės sistemos (toliau – informacinė sistema) valdytojas ir tvarkytojas – Sveikatos apsaugos ministerija (toliau – ministerija), Vilniaus g. 33, LT-01506 Vilnius. Informacinės sistemos valdytojo ir tvarkytojo atliekamos funkcijos nurodytos Lietuvos Respublikos sveikatos apsaugos ministerijos informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2012 m. balandžio 6 d. įsakymu Nr. V-312.

4. Elektroninės informacijos sauga svarbi tiek, kiek informacinė sistema svarbi ministerijos veiklai. Informacinės sistemos apimtis, automatizuotos veiklos funkcijos reglamentuojamos informacinės sistemos nuostatuose. Elektroninės informacijos saugos tikslas – užtikrinti reikiamą informacinės sistemos duomenų pasiekiamumo, vientisumo ir konfidencialumo lygį, kad informacinė sistema funkcionuotų be sutrikimų.

5. Esama informacinės sistemos saugos padėtis nustatoma periodinės rizikos analizės metu ir fiksuojama Rizikos analizės ataskaitoje.

6. Informacinės sistemos duomenų saugumo užtikrinimo prioritetinės kryptys:

6.1. informacinės sistemos konfidencialumo, pasiekiamumo ir vientisumo lygio užtikrinimas;

6.2. informacinės sistemos saugumo užtikrinimas, mokymas informacijos saugos klausimais;

6.3. efektyvus lėšų panaudojimas informacinės sistemos saugumui užtikrinti.

7. Informacinės sistemos valdytojo vadovas atsako už informacijos tvarkymo teisėtumą ir informacijos saugą.

8. Už saugos politikos įgyvendinimą atsako informacinės sistemos valdytojo paskirtas saugos įgaliotinis. Saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą informacinėje sistemoje, atlieka šias funkcijas:

8.1. teikia informacinės sistemos valdytojo vadovui pasiūlymus dėl:

8.1.1. administratorių skyrimo (saugos įgaliotinis negali atlikti administratoriaus

funkcijų);

8.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

8.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

8.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą;

8.3. teikia administratoriams privalomus vykdyti nurodymus ir pavedimus;

8.4. periodiškai inicijuoja informacinės sistemos naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problemas (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai);

8.5. atlieka kitas informacinės sistemos valdytojo pavestas ir Saugos reikalavimuose nustatytas funkcijas.

9. Už sistemos priežiūrą ir konkrečių apsaugos priemonių diegimą atsako administratorius. Administratorius atlieka šias funkcijas:

9.1. suteikia informacinės sistemos naudotojo teises;

9.2. supažindina informacinės sistemos naudotojus su informacine sistema ir juos konsultuoja;

9.3. prižiūri ir palaiko ministerijos informacinę sistemą, užtikrina efektyvų jos naudojimą;

9.4. administruoja vietinį kompiuterių ir telefonų tinklą, tarnybines stotis;

9.5. užtikrina informacijos saugojimą ir konfidencialumą, ministerijos informacinės sistemos duomenų saugą, informacinių sistemų duomenų patikimumą ir apsaugą bei saugų duomenų perdavimą tinklais, teikia pasiūlymus dėl duomenų saugos tobulinimo ministerijos saugos įgaliotiniui;

9.6. vykdo kompiuterizuotų darbo vietų priežiūrą (diegia, atnaujina programinę įrangą);

9.7. organizuoja duomenų atsarginį kopijavimą ir atsako už duomenų atkūrimą.

10. Teisės aktai, kuriais vadovaujamasi tvarkant informacinės sistemos ir šioje sistemoje tvarkomus duomenis ir užtikrinant jų saugumą:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804);

10.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (Žin., 2011, Nr. 163-7739);

10.3. Saugos reikalavimai;

10.4. Gairės;

10.5. Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866);

10.6. Lietuvos standartai LST ISO/IEC 27002:2009, LST ISO/IEC 27001:2006, taip pat kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, apibūdinantys saugų informacinės sistemos elektroninių duomenų tvarkymą;

10.7. kiti teisės aktai, reglamentuojantys informacinės sistemos duomenų tvarkymą ir elektroninių duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Sveikatos apsaugos ministerijos informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos sveikatos apsaugos ministro 2012 m. balandžio 6 d. įsakymu Nr. V-312, ir 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), ministerijos informacinė sistema priskiriama trečiai kategorijai.

12. Už informacinės sistemos rizikos vertinimo inicijavimą atsakingas saugos

įgaliotinis. Rizikos vertinimas atliekamas ne rečiau kaip kartą per metus, vadovaujantis Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos vertinimą.

13. Informacinės sistemos rizikos įvertinimas išdėstomas Rizikos analizės ataskaitoje. Rizikos analizės ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

13.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacinių technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kt.);

13.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis, duomenų pakeitimas ir sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugumo pažeidimai, vagystės ir kt.);

13.3. atsitiktinės subjektyvios aplinkybės (audra, gaisras, vandens poveikis, elektros instaliacijos gedimas, nenugalima jėga *(force majeure)* ir kt.).

14. Atsižvelgdamas į rizikos analizės ataskaitą, Lietuvos Respublikos sveikatos apsaugos ministras tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių, finansinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

15. Siekdamas užtikrinti saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, saugos įgaliotinis ne rečiau kaip kartą per 2 metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

15.1. įvertinama, ar reali duomenų sauga atitinka šiuose nuostatuose, saugos politiką įgyvendinančiuose teisės aktuose nustatytus reikalavimus;

15.2. inventorizuojama informacinės sistemos techninė ir programinė įranga;

15.3. tikrinama informacinės sistemos tarnybinėse stotyse, administratorių, naudotojų kompiuterizuotose darbo vietose įdiegta programinė įranga;

15.4. įvertinama, ar informacinės sistemos administratoriams ir naudotojams suteiktos teisės atitinka jų vykdomas funkcijas;

15.5. įvertinamas pasirengimas užtikrinti informacinės sistemos veiklos tęstinumą įvykus saugos incidentui.

16. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria jo atsakingus vykdytojus ir nustato įgyvendinimo terminus Lietuvos Respublikos sveikatos apsaugos ministras.

17. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės naudojamos tam, kad būtų užtikrintas informacinės sistemos veiklos tęstinumas ir saugus naudotojų darbas, patiriant kuo mažiau išlaidų.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

18. Prieiga prie informacinės sistemos suteikiama tik autorizuotiems naudotojams.

19. Kiekvienas informacinės sistemos naudotojas yra unikaliai identifikuojamas – naudotojas savo tapatybę patvirtina slaptažodžiu ar kita autentifikavimo priemone. Ministerijos informacinėje sistemoje naudotojui neatliekant jokių veiksmų, informacinė sistema automatiškai užsirakina.

20. Prieiga naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms vykdyti. Priimant į darbą valstybės tarnautoją ar darbuotoją, dirbantį pagal darbo sutartį (toliau – darbuotojas), ar darbuotojui keičiant pareigas, darbuotojo tiesioginis vadovas užpildo prašymą, kuriame nurodo, kokia prieiga bus reikalinga, ir šį prašymą pateikia administratoriui. Prieigos suteikimo rašytiniai prašymai turi būti saugomi tol, kol darbuotojas

dirba ministerijoje, ir metus po jo atleidimo iš darbo.

21. Prieiga galioja, kol darbuotojas dirba ministerijoje arba kol prieiga nėra atšaukta darbuotojo tiesioginio vadovo. Darbuotojų veikla informacinėje sistemoje jų atostogų metu, vykdant informacinės sistemos naudotojo veiklos tyrimą ir pan. yra ribojama. Darbuotoją atleidus iš darbo, prieiga panaikinama. Ministerijos Personalo skyrius nedelsdamas informuoja informacinės sistemos administratorius apie darbuotojo atleidimą iš darbo.

22. Ne ministerijos darbuotojui, kai tai yra būtina sutarčiai su ministerija vykdyti, prieigos suteikimo ir atšaukimo procesą sutarties vykdymo laikotarpiu inicijuoja už sutarties vykdymą atsakingas asmuo.

23. Ministerijoje turi būti naudojamos antivirusinės programos naudotojų kompiuteriuose, antivirusinės programos elektroninio pašto tarnybinėje stotyje, programinės ugniasienės naudotojų kompiuteriuose ir tinklo tarnybinėse stotyse apsaugai nuo virusų, šnipinėjimui skirtos programinės įrangos, nepageidaujamo elektroninio pašto ir pan.

24. Siekiant apsaugoti nuo žalingos programinės įrangos, ne rečiau kaip kartą per mėnesį turi būti atliekamas nuolatinis naudotojų ir tarnybinių stočių operacinių sistemų atnaujinimas.

25. Naudotojų kompiuterių apsaugos priemonės turi būti valdomos (ugniasienių įjungimas ir konfigūravimas, antivirusinių programų atnaujinimas, operacinių sistemų atnaujinimas) centralizuotai.

26. Antivirusinių programų duomenų bazės turi būti atnaujinamos periodiškai – ne rečiau kaip kartą per dieną, jei atnaujinimą pateikia antivirusinės programos gamintojas.

27. Turi būti naudojama tik legali programinė įranga, kurios sąrašą parengia ir atnaujina ministerijos Bendrųjų reikalų departamento Informacinių technologijų skyrius.

28. Ne rečiau kaip kartą per metus administratorius atlieka patikrinimą, siekdamas nustatyti, ar informacinėje sistemoje naudojama legali programinė įranga. Patikrinimą inicijuoja saugos įgaliotinis. Patikrinimo rezultatai pateikiami ministerijos Bendrųjų reikalų departamento direktoriui.

29. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų naudojant ugniasienę.

30. Konfigūruojant tinklo ugniasienes, turi būti leidžiamas tiktai būtinas organizacijos veiklai tinklo srautas.

31. Už tinklo ugniasienių administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią ugniasienių konfigūraciją atsako administratorius.

32. Tinklo ugniasienių konfigūracijos aprašymą parengia administratorius. Konfigūracijos aprašymą saugo saugos įgaliotinis. Ugniasienių konfigūracija tikrinama ne rečiau kaip kartą per metus. Tikrinimą inicijuoja saugos įgaliotinis.

33. Kompiuteriai gali būti naudojami tik informacinės sistemos naudotojų tiesioginėms pareigoms atlikti.

34. Darbuotojai kompiuteriais gali naudotis tik ministerijos patalpose, išskyrus atvejus, kai tai būtina jų tiesioginėms pareigoms atlikti.

35. Informacinės sistemos naudotojams, kai tai būtina jų tiesioginėms pareigoms atlikti, gali būti suteikiama galimybė prisijungti prie informacinės sistemos nuotoliniu būdu.

36. Nuotolinis prisijungimas turi būti autorizuotas. Naudotojų, kuriems leidžiama prisijungti nuotoliniu būdu, sąrašą rengia ir atnaujina saugos įgaliotinis.

37. Informacinėje sistemoje periodiškai (priklausomai nuo konkretaus posistemio, kad būtų užtikrinta atkūrimo galimybė) turi būti daromos atsarginės duomenų kopijos, kurios turi būti laikomos atskiroje patalpoje.

38. Atkūrimo iš atsarginių kopijų galimybė tūri būti tikrinama ne rečiau kaip kartą per metus. Atkūrimo galimybės išbandymą inicijuoja saugos įgaliotinis.

39. Saugos įgaliotinis atsako už tai, kad būtų užtikrinta:

39.1. informacinės sistemos pagrindinių funkcijų atkūrimo per 8 val. nuo veiklos sutrikimo galimybė;

39.2. informacinės sistemos prieinamumas ne mažiau kaip 90 proc. darbo laiko.

40. Ministerijos informacinės sistemos duomenų tvarkymo ir saugumo procedūros išdėstomos Saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

41. Saugos įgaliotinis privalo turėti informacinių technologijų specialisto kvalifikaciją, išmanyti informacinių sistemų administravimą, gerai žinoti elektroninės informacijos saugos principus bei saugos užtikrinimo metodus.

42. Informacinės sistemos administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos principus, darbą su duomenų perdavimo tinklais, duomenų bazių administravimo ir priežiūros pagrindus.

43. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti informacinės sistemos duomenis Lietuvos Respublikos sveikatos apsaugos ministro nustatyta tvarka ir būti susipažinę su Informacinės sistemos nuostatais, šiais nuostatais ir kitais informacinės sistemos saugą reglamentuojančiais teisės aktais.

44. Informacinės sistemos naudotojams turi būti periodiškai rengiami informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Mokymus organizuoja saugos įgaliotinis.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

45. Saugos įgaliotinis pasirašytinai supažindina informacinės sistemos naudotojus su šiais nuostatais ir kitais informacinės sistemos saugą reglamentuojančiais teisės aktais ir informuoja apie šių teisės aktų pakeitimus.

VI. BAIGIAMOSIOS NUOSTATOS

46. Informacinės sistemos naudotojai, pažeidę šiuos nuostatus, atsako teisės aktų nustatyta tvarka.

_____