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

DĖL ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. spalio 7 d. Nr. V-889
Vilnius

Vadovaudamasis Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimo Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo“ (Žin., 2011, Nr. 113-5318) 3.1 punktu ir Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891; 2011, Nr. 55-2642), 6.1, 7 ir 8 punktais:

1. T v i r t i n u Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatus (pridedama).

2. N u s t a t a u, kad:

2.1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos pagrindinio tvarkytojo valstybės įmonės Registrų centro direktorius per 3 mėnesius nuo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo paskiria Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos vyriausiąjį saugos įgaliotinį;

2.2. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos pagrindinis tvarkytojas valstybės įmonė Registrų centras per 6 mėnesius nuo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo parengia ir pateikia Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos valdytojui tvirtinti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos veiklos tęstinumo valdymo plano ir Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudotojų administravimo taisyklių projektus.

3. P a v e d u įsakymo vykdymą kontroliuoti ministerijos kancleriui.

SVEIKATOS APSAUGOS MINISTRAS RAIMONDAS ŠUKYS

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2011-08-01 raštu Nr. 1D-5307 (3)

SUDERINTA
Valstybės įmonės Registrų centro
2011-07-26 raštu Nr. (1.1.5.)s-3231

PATVIRTINTA
Lietuvos Respublikos
sveikatos apsaugos ministro
2011 m. spalio 7 d. įsakymu Nr. V-889

ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (toliau – ESPBI IS) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja ESPBI IS duomenų saugą ir apibrėžia ESPBI IS saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka ESPBI IS nuostatuose, 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), Saugos dokumentų turinio gairėse, patvirtintose Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), Bendruosiuose reikalavimuose organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintuose Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) (Žin., 2008, Nr. 135-5298), ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006 vartojamas sąvokas.

3. ESPBI IS duomenų saugos tikslas – užtikrinti ESPBI IS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. ESPBI IS duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos lygio kėlimo, saugos priemonių projektavimo ir diegimo principus.

4. ESPBI IS informacijos saugos užtikrinimo prioritetinės kryptys:

4.1. paciento asmens ir ypatingų sveikatos duomenų, registracijos ir siuntimų konsultuoti, tirti, gydyti duomenų konfidencialumo, vientisumo ir prieinamumo užtikrinimas naudojant technines, organizacines ir teisines priemones:

4.1.1. duomenų konfidencialumas užtikrinamas techninėmis ir organizacinėmis priemonėmis ribojant priėjimą prie asmens duomenų ir ypatingų asmens duomenų; priėjimas suteikiamas tik teisėtiems ESPBI IS tvarkytojams ir naudotojams, kurių tapatybė yra nustatyta, ir tik prie duomenų, būtinų ESPBI IS naudotojo veiklos funkcijoms vykdyti; supažindinant ESPBI IS administratorius ir ESPBI IS naudotojus su konfidencialaus asmens duomenų tvarkymo principais;

4.1.2. duomenų ar sistemos vientisumas užtikrinamas valdant teisėtą duomenų ar sistemos keitimą, kontroliuojant duomenų įvedimą, stebint ir reaguojant į galimą neteisėtą duomenų ar sistemos keitimą ar sunaikinimą; atsakingi už duomenų įvedimą ar keitimą sistemos ESPBI IS administratoriai ir ESPBI IS naudotojai supažindinami su klaidų ir vientisumo pažeidimo nustatymo ir koregavimo metodais ir tvarkų aprašais;

4.1.3. duomenų ar sistemos prieinamumas užtikrinamas organizacinėmis ir technologinėmis priemonėmis valdant ESPBI IS, jos elementų ar duomenų keitimus, naudojant perteklines ar alternatyvias informacinių sistemų ir duomenų tinklų technologines priemones, atliekant ESPBI IS atkūrimo plano bandymus ir veiklos tęstinumo valdymo plano bandymus;

4.2. kitos prioritetinės kryptys:

4.2.1. administracinių saugaus darbo su duomenimis, asmens duomenimis ir ypatingais

asmens duomenimis priemonių įgyvendinimas ir kontrolė (ESPBI IS duomenų gavėjų ir teikėjų, ESPBI IS tvarkytojų teisių, įpareigojimų, atsakomybės ribų, detalių ESPBI IS elektroninės informacijos tvarkymo ir administravimo taisyklių nustatymas);

4.2.2. technologinė elektroninės informacijos apdorojimo priemonių (ESPBI IS tarnybinių stočių saugojimo patalpų, tarnybinių stočių, elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga.

5. Saugos nuostatai taikomi ESPBI IS valdytojui, ESPBI IS tvarkytojams, ESPBI IS saugos įgaliotiniams, ESPBI IS administratoriams ir ESPBI IS naudotojams.

6. ESPBI IS valdytoja – Sveikatos apsaugos ministerija (toliau – SAM), adresas: Vilniaus g. 33, LT-01506 Vilnius:

6.1. organizuoja ir vadovauja ESPBI IS veiklai;

6.2. rengia ir tvirtina teisės aktus, susijusius su ESPBI IS tvarkymu ir duomenų sauga, ir prižiūri, kaip jų laikomasi;

6.3. priima sprendimą dėl ESPBI IS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

6.4. kontroliuoja, kad ESPBI IS būtų tvarkoma vadovaujantis Lietuvos Respublikos valstybės įstatymais, Saugos nuostatais ir kitais teisės aktais.

7. Pagrindinis ESPBI IS tvarkytojas – valstybės įmonė Registrų centras (toliau – RC), adresas: V. Kudirkos g. 18, LT-03105 Vilnius:

7.1. skiria ESPBI IS vyriausiąjį saugos įgaliotinį;

7.2. skiria ESPBI IS administratorių arba kelis ESPBI IS administratorius, vykdančius atskiras ESPBI IS administravimo funkcijas (toliau – RC ESPBI IS administratorius);

7.3. pagal kompetenciją rengia teisės aktų, susijusių su ESPBI IS tvarkymu ir duomenų sauga, projektus;

7.4. atlieka ESPBI IS duomenų bazių priežiūrą;

7.5. užtikrina ESPBI IS sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.6. užtikrina nepertraukiamą ESPBI IS veikimą ir duomenų, esančių ESPBI IS duomenų bazėse, saugą;

7.7. ESPBI IS valdytojo ir ESPBI IS duomenų gavėjų sutarčių dėl duomenų teikimo nustatyta tvarka automatiškai teikia ESPBI IS duomenis duomenų gavėjams bei užtikrina duomenų saugą iki duomenys pasiekia duomenų gavėją sutartyse numatytomis sąlygomis ir tvarka;

7.8. atlieka kitas ESPBI IS nuostatų, Saugos nuostatų, Saugos reikalavimų ir kitų teisės aktų nustatytas funkcijas.

8. ESPBI IS tvarkytojos – sveikatinimo veiklą vykdančios įstaigos (toliau – SĮ), tvarkančios ESPBI IS duomenis:

8.1. kiekviena paskiria ESPBI IS administratorių atlikti ESPBI IS administravimo funkcijas savo įstaigoje;

8.2. kiekviena paskiria ESPBI IS saugos įgaliotinį savo įstaigoje. SĮ ESPBI IS administratoriai negali vykdyti ESPBI IS saugos įgaliotinio funkcijų;

8.3. pagal kompetenciją rengia ir tvirtina dokumentus, susijusius su ESPBI IS tvarkymu ir duomenų sauga SĮ, ir prižiūri, kaip jų laikomasi;

8.4. užtikrina SĮ ESPBI IS tvarkomų duomenų saugą;

8.5. užtikrina SĮ ESPBI IS naudotojų darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių duomenų saugą, diegimą ir priežiūrą;

8.6. atlieka kitas Saugos nuostatų, Saugos reikalavimų, ESPBI IS nuostatų ir kitų teisės aktų nustatytas funkcijas.

9. ESPBI IS vyriausiasis saugos įgaliotinis:

9.1. įgyvendina ESPBI IS duomenų saugą, vadovaudamasis Saugos reikalavimais;

9.2. atsako už ESPBI IS saugos dokumentų reikalavimų vykdymą;

9.3. teikia ESPBI IS valdytojui siūlymus dėl:

9.3.1. saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.3.2. ESPBI IS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

9.4. teikia pagrindinio ESPBI IS tvarkytojo vadovui siūlymus dėl RC ESPBI IS administratorių paskyrimo;

9.5. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

9.6. pagal kompetenciją teikia RC ESPBI IS administratoriams, SĮ ESPBI IS saugos įgaliotiniams privalomus vykdyti nurodymus ir pavedimus, koordinuoja SĮ ESPBI IS saugos įgaliotinių veiklą;

9.7. pasirašytinai supažindina RC ESPBI IS administratorius, SĮ ESPBI IS saugos įgaliotinius su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą;

9.8. kasmet organizuoja SĮ ESPBI IS saugos įgaliotinių, ESPBI IS administratorių, ESPBI IS naudotojų (išskyrus SĮ ESPBI IS naudotojus) kvalifikacijos tobulinimą duomenų saugos klausimais, reguliariai jiems primena saugos problemas (elektroniniu paštu, parengia atmintines naujai priimtiems darbuotojams ir pan.);

9.9. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

10. SĮ ESPBI IS saugos įgaliotiniai:

10.1. įgyvendina ESPBI IS duomenų saugą SĮ;

10.2. atsako už ESPBI IS saugos dokumentų reikalavimų vykdymą SĮ;

10.3. teikia ESPBI IS vyriausiajam saugos įgaliotiniui siūlymus dėl:

10.3.1. Saugos nuostatų bei saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

10.3.2. atitikties Saugos reikalavimams vertinimo atlikimo SĮ;

10.4. koordinuoja elektroninės informacijos saugos incidentų tyrimą SĮ;

10.5. teikia informaciją, susijusią su ESPBI IS duomenų sauga SĮ, ESPBI IS vyriausiajam saugos įgaliotiniui (jam paprašius);

10.6. pasirašytinai supažindina SĮ ESPBI IS administratorius, SĮ ESPBI IS naudotojus su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą;

10.7. vertina SĮ ESPBI IS naudotojų pasirengimą darbui su ESPBI IS;

10.8. kasmet organizuoja SĮ ESPBI IS naudotojų kvalifikacijos tobulinimą duomenų saugos klausimais, reguliariai jiems primena saugos problemas (elektroniniu paštu, parengia atmintines naujai priimtiems darbuotojams ir pan.);

10.9. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir kitus ESPBI IS vyriausiojo saugos įgaliotinio nurodymus, susijusius su ESPBI IS duomenų sauga;

10.10. registruoja elektroninės informacijos saugos incidentus, informuoja apie juos ESPBI IS vyriausiąjį saugos įgaliotinį ir teikia siūlymus dėl minėtų incidentų pašalinimo.

11. RC ESPBI IS administratorius:

11.1. atsako už ESPBI IS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą;

11.2. registruoja ESPBI IS naudotojus ir suteikia prieigos teisę naudotis ESPBI IS infrastruktūra paskirtoms funkcijoms atlikti;

11.3. pagal kompetenciją rengia pasiūlymus dėl ESPBI IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

11.4. atlieka ESPBI IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų), esančių RC patalpose, administravimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį ESPBI IS saugos politiką įgyvendinančių dokumentų reikalavimams.

12. SĮ ESPBI IS administratorius:

12.1. atsako už SĮ patalpose esančios ir darbui su ESPBI IS naudojamos techninės ir programinės įrangos, infrastruktūros administravimą;

12.2. pagal kompetenciją rengia pasiūlymus dėl ESPBI IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

12.3. atlieka ESPBI IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų), esančių SĮ patalpose, administravimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį ESPBI IS saugos politiką įgyvendinančių dokumentų reikalavimams.

13. ESPBI IS naudotojai:

13.1. vadovaudamiesi Saugos nuostatais, ESPBI IS saugaus elektroninės informacijos tvarkymo taisyklėmis, ESPBI IS naudotojų administravimo taisyklėmis, pareigybių aprašymais ir kitais teisės aktais, naudojasi ESPBI IS informacijos tvarkymo arba kitais su tiesioginių funkcijų vykdymu susijusiais tikslais;

13.2. informuoja SĮ, veikiančios kaip ESPBI IS tvarkytojas, ESPBI IS saugos įgaliotinį apie elektroninės informacijos saugos incidentus, o šios įstaigos ESPBI IS administratorių apie ESPBI IS darbo sutrikimus;

13.3. vykdo kitas Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su ESPBI IS naudojimu ir ESPBI IS duomenų sauga;

13.4. atsako už tvarkomų duomenų saugą teisės aktų nustatyta tvarka.

14. Tvarkant ESPBI IS duomenis ir užtikrinant saugą vadovaujamasi šiais teisės aktais:

14.1. Lietuvos Respublikos sveikatos sistemos įstatymu (Žin., 1994, Nr. 63-1231; 1998, Nr. 112-3099);

14.2. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu (Žin., 1996, Nr. 66-1572; 1998, Nr. 109-2995);

14.3. Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymu (Žin., 1996, Nr. 102-2317; 2009, Nr. 145-6425);

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

14.5. Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais;

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

14.7. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms;

14.8. Lietuvos standartais LST ISO/IEC 27002:2009, LST ISO/IEC 27001:2006, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, reglamentuojančiais saugų duomenų tvarkymą;

14.9. Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą, ESPBI IS tvarkytojų veiklą bei duomenų saugos valdymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymu Nr. 1V-247 (Žin., 2007, Nr. 78-3160), 3.2.1 bei 3.2.7 punktais, ESPBI IS priskirtina antrai informacinių sistemų kategorijai.

16. ESPBI IS saugos priemonės parenkamos įvertinus galimus rizikos veiksnius ESPBI IS duomenų vientisumui, konfidencialumui ir prieinamumui.

17. ESPBI IS kaupiamų ir apdorojamų duomenų rinkimo tvarka, kriterijai bei sąrašas

pateikiami ESPBI IS nuostatuose.

18. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugojimo priemonėms, atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ESPBI IS duomenys priskiriami antrajam saugumo lygiui.

19. ESPBI IS vyriausiasis saugos įgaliotinis, ESPBI IS valdytojui informavus, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja ESPBI IS rizikos įvertinimą. Prireikus ESPBI IS vyriausiasis saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. ESPBI IS rizikos veiksnių įvertinimas atliekamas kokybiniu rizikos vertinimo metodu. Atliekant rizikos įvertinimą turi būti vertinamos rizikos, susijusios su:

19.1. ESPBI IS tarnybinėmis stotimis ir jų valdymu;

19.2. duomenų perdavimo tinklu, kuriuo teikiami ir gaunami duomenys iš registrų, informacinių sistemų ir klasifikatorių;

19.3. duomenų perdavimo tinklu, kuriuo teikiami ir gaunami duomenys toliau esantiems ESPBI IS naudotojams;

19.4. ESPBI IS naudotojų darbo vietomis.

20. ESPBI IS rizikos įvertinimas pateikiamas Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos ESPBI IS informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

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

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis duomenims gauti, duomenų pakeitimas ir sunaikinimas, informacinių technologijų duomenų perdavimo tinklais trikdymai, saugos pažeidimai, vagystės ir kt.);

20.3. nenugalimos jėgos (*force majeure*) (audros, gaisrai, vandens poveikis ir kt.).

21. ESPBI IS valdytojas ESPBI IS rizikos įvertinimą gali pavesti (įgalioti) atlikti trečiajai šaliai.

22. Atsižvelgdamas į ESPBI IS rizikos įvertinimo ataskaitą, ESPBI IS valdytojas tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

23. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikos, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 (Žin., 2004, Nr. 80-2855), nustatyta tvarka ESPBI IS vyriausiasis saugos įgaliotinis kasmet organizuoja ESPBI IS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

23.1. įvertinama saugos dokumentų ir realios duomenų saugos situacijos atitiktis saugos politiką apibrėžiantiems dokumentams;

23.2. inventorizuojama ESPBI IS techninė ir programinė įranga;

23.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų ESPBI IS naudotojų kompiuterinių darbo vietų ir visos tarnybinėse stotyse įdiegtos programos ir jų sąranka;

23.4. patikrinama ESPBI IS naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

23.5. įvertinamas pasirengimas užtikrinti ESPBI IS tęstinumą įvykus saugos incidentui.

24. ESPBI IS valdytojas ESPBI IS saugos atitikties vertinimą gali pavesti (įgalioti) atlikti trečiajai šaliai.

25. Atlikus ESPBI IS informacinių technologijų saugos atitikties vertinimą, parengiamas ir sveikatos apsaugos ministro įsakymu patvirtinamas pastebėtų trūkumų šalinimo planas, paskiriami atsakingi vykdytojai ir nustatomi įgyvendinimo terminai.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. ESPBI IS duomenų gavėjai privalo užtikrinti gaunamų ESPBI IS duomenų saugą antros kategorijos informacinių sistemų saugai keliamu lygiu.

27. ESPBI IS duomenų saugos techninės ir programinės priemonės:

27.1. patalpų įrengimas ir apsauga: įrengiama atskira tarnybinių stočių patalpa su įėjimo kontrolės sistema, signalizacija, užtikrinama bendra pastato apsauga;

27.2. kompiuterinės technikos apsauga: serveriai dubliuoja svarbias funkcijas, taikomos duomenų, saugomų magnetiniuose diskuose, specialiosios apsaugos priemonės (RAID), užtikrinamas nuotolinis serverių valdymas ir gedimų diagnozavimas, užtikrinama visų tarnybinių stočių gedimų prevencija, įrengiamas įžeminimas, nepertraukiamo maitinimo šaltiniai, avariniai generatoriai, sudaromos reikiamos eksploatavimo sąlygos, įrengiama nuolat veikianti techninio aptarnavimo telefono linija ir kt.;

27.3. naudojama tik legali programinė įranga;

27.4. tarnybinėse stotyse nėra programinės įrangos, nesusijusios su ESPBI IS duomenų tvarkymu, ESPBI IS naudotojų ir programinės įrangos administravimu;

27.5. ESPBI IS naudotojų darbo vietose veikia programinė įranga, skirta kovai su kenksminga programine įranga, automatiškai atnaujinama ne rečiau kaip kas tris dienas;

27.6. pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

27.6.1. duomenų saugai užtikrinti daromos pagrindinės duomenų bazės atsarginės duomenų kopijos;

27.6.2. atsarginės kopijos daromos magnetinėse laikmenose;

27.6.3. atsarginės kopijos magnetinėse laikmenose daromos reguliariai, kiekvieną darbo dieną;

27.6.4. sukurta atsarginė kopija pažymima specialia ženklinimo etikete, kurioje nurodoma kopijavimo data, kopiją padariusio asmens duomenys (pareigos, vardas, pavardė), duomenų katalogai;

27.6.5. kiekvienos savaitės paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra savaitinė kopija;

27.6.6. kiekvieno mėnesio paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra mėnesinė kopija;

27.6.7. kiekvienų metų paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra metinė kopija;

27.6.8. atsargines dokumentų kopijas turi teisę daryti tik RC ESPBI IS administratorius, kurio pareigybės aprašyme numatyta ši funkcija;

27.6.9. darant (padarius) atsargines kopijas, būtina užtikrinti kopijų kokybę;

27.6.10. atsarginės kopijos magnetinėje laikmenoje saugomos RC duomenų kopijų archyve. Už jų atidavimą saugoti atsako RC ESPBI IS administratorius, vykdantis dokumentų kopijavimo funkciją;

27.6.11. atsarginės metinės kopijos saugomos 10 metų nuo jų sukūrimo dienos. Atsarginės mėnesinės kopijos saugomos 1 metus nuo jų sukūrimo dienos. Atsarginės savaitinės kopijos saugomos 1 mėnesį nuo jų sukūrimo dienos;

27.6.12. ESPBI IS duomenų atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik RC ESPBI IS administratorius;

27.6.13. kopijų, iš kurių būtų galima atkurti ESPBI IS duomenis, darymo ir saugojimo tvarka turi būti detaliai aprašyta ESPBI IS saugaus elektroninės informacijos tvarkymo taisyklėse.

28. ESPBI IS naudotojų identifikavimas:

28.1. ESPBI IS naudotojai identifikuojami naudojant elektroninio parašo kvalifikuotą sertifikatą ir (arba) slaptažodį;

28.2. ESPBI IS naudotojų administravimo taisyklėse nustatomi specialūs slaptažodžių

sistemos reikalavimai (periodinis privalomas slaptažodžių keitimas, slaptažodžio ilgio apribojimai ir kt.);

28.3. ESPBI IS naudotojų duomenys tvarkomi ESPBI IS saugos posistemėje, ESPBI IS naudotojų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi ESPBI IS audito posistemėje. ESPBI IS naudotojų ir su jais susijusių duomenų tvarkymas detaliai aprašytas ESPBI IS naudotojų administravimo taisyklėse.

29. Apsauga nuo galimų tyčinių ESPBI IS naudotojų veiksmų:

29.1. nustatomi ESPBI IS naudotojų vaidmenys ir jiems priskiriami konkretūs leidžiami atlikti veiksmai;

29.2. ribojama ESPBI IS naudotojo teisė manipuliuoti duomenimis;

29.3. ESPBI IS naudotojo teisės suteikiamos ir sustabdomos įstaigos, kurioje dirba naudotojas, vadovo prašymu;

29.4. visi ESPBI IS naudotojo prisijungimai prie ESPBI IS registruojami ESPBI IS prisijungimų žurnale ir saugomi 3 metus;

29.5. visi pakeitimai duomenų bazėje yra registruojami elektroniniame žurnale;

29.6. įdiegiama speciali techninė įranga, registruojanti į atskirą žurnalą išorinėje sistemoje administratoriaus atliekamus veiksmus duomenų bazėje.

30. Nešiojamieji kompiuteriai, jei juose yra įdiegta ESPBI IS naudotojo darbo vietos programinė įranga, gali būti išnešami iš įstaigos, kuriai priskirta ESPBI IS naudotojo darbo vieta, patalpų tik vadovaujantis įstaigos direktoriaus įsakymu patvirtintu kompiuterių ir programinės įrangos ir informacinių resursų naudojimo darbo vietose tvarkos aprašu. Šiuo atveju ESPBI IS naudotojas asmeniškai Lietuvos Respublikos teisės aktų nustatyta tvarka atsako už kompiuterio duomenų saugojimo laikmenose esančių ESPBI IS duomenų saugą.

31. ESPBI IS duomenų saugos administracinės priemonės:

31.1. veiksmai, užtikrinantys duomenų saugą, nustatomi ESPBI IS naudotojų pareigybių aprašymuose;

31.2. ESPBI IS naudotojai supažindinami su galiojančiais norminiais aktais, reglamentuojančiais duomenų saugą;

31.3. ESPBI IS naudotojų atsakomybę nustato pasirašomi asmeniniai ESPBI IS naudotojų pasižadėjimai;

31.4. parengiamas ESPBI IS duomenų pažeidimo rizikos valdymo priemonių planas;

31.5. duomenų saugos dokumentai atnaujinami ne rečiau kaip kartą per metus (atlikus ESPBI IS rizikos įvertinimą ar ESPBI IS informacinių technologijų saugos atitikties vertinimą ar pasikeitus teisės aktams, reglamentuojantiems duomenų saugą).

32. ESPBI IS duomenų apsaugos programinės priemonės:

32.1. tarnybinėse stotyse ir darbo vietose naudojama tik licencijuota nuolat atnaujinama programinė įranga;

32.2. naudojamos užkardos;

32.3. tarnybinėse stotyse ir darbo vietose naudojama nuolat atnaujinama antivirusinė programinė įranga;

32.4. darbo vietose, kuriose yra įdiegta prieiga prie ESPBI IS, gali būti naudojamos tik legalios programos ir dokumentai, susiję su ESPBI IS naudotojo funkcijomis.

33. ESPBI IS programiniai kodai privalo būti apsaugoti nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

34. ESPBI IS telekomunikacinio tinklo apsaugos priemonės:

34.1. tinklo segmentavimas;

34.2. prieigos kontrolės sąrašai (ACL);

34.3. „statefull“ ugniasienė; tinklo išorinis perimetras apsaugotas interneto prieigos maršruto parinktuvu ir ugniasiene. Išoriniam perimetrui apsaugoti naudojamas statinis 7 lygmens pagal OSI modelį paketų ir „statefull“ (sekantis paketų būsenas) filtravimas;

34.4. tinklo adresų transliavimas (NAT/PAT);

34.5. pagrindinė ESPBI IS duomenų pateikimo prieiga yra duomenų perdavimas

duomenų perdavimo kanalu, panaudojant saugų HTTPS protokolą. ESPBI IS naudotojai identifikuojami ir jiems suteikiamos teisės pagal jam suteiktą naudotojo vardą ir slaptažodį. Kaip papildoma priemonė, ribojanti prisijungimą prie ESPBI IS, yra interneto protokolo (angl. IP) adresų filtravimas.

35. ESPBI IS duomenys, perduodami ne per ESPBI IS tvarkytojams priklausančias duomenų perdavimo linijas, privalo būti šifruojami.

36. Papildomi reikalavimai ESPBI IS techninėms ir organizacinėms informacijos saugos valdymo priemonėms gali atsirasti atlikus eilinę rizikos analizę arba pasikeitus teisės aktams, reglamentuojantiems duomenų saugą informacinėse sistemose.

IV. REIKALAVIMAI PERSONALUI

37. ESPBI IS vyriausiasis saugos įgaliotinis ir SĮ ESPBI IS saugos įgaliotiniai privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Saugos reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais ESPBI IS duomenų tvarkymą, standartais bei kitais dokumentais, sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

38. ESPBI IS administratoriai privalo turėti darbo su kompiuterių tinklais patirties, mokėti užtikrinti jų saugą, taip pat turėti sisteminių programinių priemonių administravimo bei priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

39. ESPBI IS naudotojai privalo turėti darbo su kompiuteriu įgūdžių, mokėti tvarkyti ESPBI IS duomenis ESPBI IS nuostatų nustatyta tvarka ir būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

40. ESPBI IS naudotojų mokymus informacijos saugos klausimais kasmet inicijuoja vyriausiasis ESPBI IS saugos įgaliotinis. SĮ ESPBI IS naudotojų mokymus organizuoja SĮ ESPBI IS saugos įgaliotiniai, kitų ESPBI IS naudotojų mokymus organizuoja vyriausiasis ESPBI IS saugos įgaliotinis.

41. ESPBI IS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti sveikatinimo veiklą vykdančios įstaigos, veikiančios kaip ESPBI IS tvarkytojas, ESPBI IS saugos įgaliotiniui ir (ar) ESPBI IS administratoriui.

42. Įvykus elektroninės informacijos saugos incidentui, nenumatytai situacijai, ESPBI IS saugos įgaliotinių, ESPBI IS administratorių, ESPBI IS naudotojų veiksmus reglamentuoja ESPBI IS veiklos tęstinumo valdymo planas.

V. ESPBI IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

43. Tvarkyti ESPBI IS duomenis gali tik tie ESPBI IS naudotojai, kurie yra susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

44. Saugos nuostatus ir saugos politiką įgyvendinančius dokumentus SĮ direktorius gauna sutarties dėl ESPBI IS duomenų tvarkymo pasirašymo metu. Už SĮ ESPBI IS naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais atsako SĮ ESPBI IS saugos įgaliotiniai.

45. Už kitų ESPBI IS naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais atsako ESPBI IS vyriausiasis saugos įgaliotinis.

VI. SAUGOS NUOSTATŲ ATNAUJINIMO TVARKA

46. Saugos nuostatai ir kiti ESPBI IS saugos politiką įgyvendinantys dokumentai iš esmės persvarstomi ir prireikus keičiami ne rečiau kaip kartą per metus, atlikus ESPBI IS duomenų saugos rizikos įvertinimą.

47. Apie Saugos nuostatų ar kitų ESPBI IS saugos politiką įgyvendinančių dokumentų pripažinimą netekusiais galios, keitimą ar priėmimą ESPBI IS vyriausiasis saugos įgaliotinis nedelsdamas informuoja ESPBI IS naudotojus.

VII. BAIGIAMOSIOS NUOSTATOS

48. ESPBI IS valdytojas, ESPBI IS tvarkytojai, ESPBI IS saugos įgaliotiniai, ESPBI IS administratoriai ir ESPBI IS naudotojai, pažeidę Saugos nuostatų arba kitų saugų duomenų tvarkymą reglamentuojančių teisės aktų reikalavimus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.

_____