VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS
DIREKTORIAUS
Į S A K Y M A S

DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS EUROPOS SĄJUNGOS SOCIALINĖS APSAUGOS DUOMENŲ MAINŲ INFORMACINĖS SISTEMOS NUOSTATŲ IR ŠIOS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2012 m. gruodžio 20 d. Nr. 1K-338
Vilnius

Vadovaudamasis Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. balandžio 19 d. nutarimu Nr. 451 (Žin., 2004, Nr. 58-2061), 8 punktu, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo (Žin., 2011, Nr. 163-7739) 8 straipsniu 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), 6 ir 8 punktais:

1. T v i r t i n u pridedamus:

1.1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos nuostatus (neskelbiami);

1.2. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos duomenų saugos nuostatus.

2. Neskelbiama.

3. Neskelbiama.

4. Neskelbiama.

DIREKTORIUS ALGIS SASNAUSKAS

SUDERINTA
Valstybinės duomenų apsaugos inspekcijos
2012-12-03 raštu Nr. 2R-4386 (3.33)

SUDERINTA
Informacinės visuomenės plėtros komiteto
prie Susisiekimo ministerijos
2012-11-14 raštu Nr. S-1612

SUDERINTA
Lietuvos Respublikos vidaus reikalų
ministerijos
2012-11-07 raštu Nr. 1D-7391 (52)

SUDERINTA
Lietuvos Respublikos sveikatos apsaugos
ministerijos
2012-09-28 raštu Nr. (14.4-29)10-7937

PATVIRTINTA
Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2012 m. gruodžio 20 d. įsakymu Nr. 1K-338

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS EUROPOS SĄJUNGOS SOCIALINĖS APSAUGOS DUOMENŲ MAINŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos nuostatų (toliau – Saugos nuostatai) tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai rinkti, apdoroti, kaupti, saugoti Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos (toliau – EDMIS) duomenis, teikti juos suinteresuotiems juridiniams ir fiziniams asmenims.

2. Saugos nuostatai parengti pagal Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus, patvirtintus Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45; 2007, Nr. 49-1891), Saugos dokumentų turinio gaires, patvirtintas Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninius saugos reikalavimus, patvirtintus Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866), Bendruosius reikalavimus organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintus Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) (Žin., 2008, Nr. 135-5298).

3. Saugos nuostatuose vartojamos sąvokos atitinka Saugos nuostatų 2 punkte išvardintuose teisės aktuose bei Lietuvos standarte LST ISO/IEC 27001: 2006 vartojamas sąvokas.

4. EDMIS saugos politiką (toliau – saugos politika) apima Saugos nuostatai, EDMIS saugaus elektroninės informacijos tvarkymo taisyklės, EDMIS veiklos tęstinumo valdymo planas, EDMIS naudotojų administravimo taisyklės, kiti teisės aktai, reglamentuojantys EDMIS duomenų tvarkymo teisėtumą ir saugos valdymą.

5. EDMIS saugos tikslas – užtikrinti EDMIS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. EDMIS duomenų saugumui užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti elektroninės informacijos saugos principus.

6. EDMIS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1. EDMIS duomenims tvarkyti naudojamos techninės ir programinės įrangos bei duomenų tvarkymo kontrolė;

6.2. fizinė elektroninės informacijos apdorojimo priemonių (VLK, Teritorinių ligonių kasų (toliau – TLK) ir Lietuvos Respublikos sveikatos apsaugos ministerijos (toliau – SAM) patalpos, tarnybinės stotys, elektroninės informacijos perdavimo įranga, programinė įranga) apsauga;

6.3. organizacinių saugaus darbo su duomenimis priemonių įgyvendinimas ir kontrolė (nustatomos EDMIS tvarkytojų ir EDMIS duomenų gavėjų teisės, įpareigojimai, atsakomybės ribos, detalios EDMIS elektroninės informacijos tvarkymo ir administravimo taisyklės).

7. Saugos nuostatai taikomi visiems EDMIS tvarkytojų atsakingiems asmenims ir EDMIS naudotojams, saugos įgaliotiniui, administratoriams, EDMIS duomenų gavėjams.

8. EDMIS valdytoja ir pagrindinė tvarkytoja yra VLK, buveinės adresas – Europos

aikštė 1, LT-03505 Vilnius.

9. EDMIS tvarkytojai regionuose – TLK:

9.1. Vilniaus TLK, buveinės adresas – Ž. Liauksmino g. 6, LT-01101 Vilnius, ir Naujoji g. 48 (III a.), Alytus;

9.2. Kauno TLK, buveinės adresas – Aukštaičių g. 10, LT-44147 Kaunas, ir P. Kriaučiūno g. 2, LT- 68263 Marijampolė;

9.3. Klaipėdos TLK, buveinės adresas – Pievų Tako g. 38, LT-91220 Klaipėda, ir Prezidento g. 7, LT-72253 Tauragė;

9.4. Šiaulių TLK, buveinės adresas – Vilniaus g. 273, LT-76332 Šiauliai, ir Kalno g. 40, LT-87134 Telšiai;

9.5. Panevėžio TLK, buveinės adresas – Respublikos g. 66, LT-35158 Panevėžys, ir Aušros g. 80, LT-28181 Utena.

10. EDMIS tvarkytoja, dirbant su jos kompetencijai priskirtais ES socialinės apsaugos dokumentais, yra SAM, buveinės adresas – Vilniaus g. 33, LT-01506 Vilnius.

11. EDMIS tvarkytojais paslaugų teikimo laikotarpiui gali būti paskirti ir tretieji asmenys, VLK teikiantys EDMIS diegimo, priežiūros ir vystymo paslaugas pagal paslaugų teikimo sutartį.

12. EDMIS valdytojo ir EDMIS tvarkytojų funkcijos nurodytos EDMIS nuostatuose.

13. EDMIS valdytojas rengia ir tvirtina šiuos saugos politiką įgyvendinančius dokumentus:

13.1. Saugaus EDMIS elektroninės informacijos tvarkymo taisykles (toliau – Tvarkymo taisyklės);

13.2. EDMIS veiklos tęstinumo valdymo planą (toliau – Valdymo planas);

13.3. EDMIS naudotojų administravimo taisykles (toliau – Administravimo taisyklės).

14. VLK vadovas įsakymu skiria EDMIS saugos įgaliotinį (toliau – Saugos įgaliotinis), tvirtina Saugos nuostatus, suderintus su Lietuvos Respublikos vidaus reikalų ministerija, Tvarkymo taisykles, Valdymo planą, Administravimo taisykles. VLK prižiūri EDMIS saugos politiką reglamentuojančių teisės aktų parengimą ir įgyvendinimą.

15. VLK vadovas turi:

15.1. pavesti Saugos įgaliotiniui organizuoti ir kontroliuoti saugos politiką reglamentuojančių teisės aktų įgyvendinimą VLK, TLK ir SAM;

15.2. paskirti EDMIS administratorius, pavesti jiems užtikrinti EDMIS tarnybinių stočių saugų funkcionavimą, administruoti EDMIS duomenų bazes Saugos nuostatų ir kitų saugos politiką reglamentuojančių teisės aktų nustatyta tvarka.

16. TLK ir SAM vadovai turi paskirti atsakingus asmenis ir pavesti jiems tvarkyti EDMIS duomenis, užtikrinti EDMIS duomenų saugą saugos politiką reglamentuojančių teisės aktų nustatyta tvarka.

17. EDMIS duomenų saugą organizuoja Saugos įgaliotinis, VLK vadovo įsakymu paskirtas atsakingu už duomenų saugą.

18. Saugos įgaliotinis, įgyvendindamas EDMIS saugą, atlieka šias funkcijas:

18.1. teikia VLK vadovui pasiūlymus dėl:

18.1.1. EDMIS administratorių paskyrimo (Saugos įgaliotinis negali atlikti administratoriaus funkcijų);

18.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

18.1.3. EDMIS saugos reikalavimų atitikties vertinimo atlikimo;

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

18.3. teikia EDMIS administratoriams privalomus vykdyti nurodymus ir pavedimus;

18.4. informuoja EDMIS tvarkytojus apie EDMIS saugos problematiką;

18.5. atsako už EDMIS saugos politikos įgyvendinimo organizavimą;

18.6. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas ir vykdo kitus, susijusius su EDMIS sauga, EDMIS

valdytojo nurodymus.

19. EDMIS administratorių funkcijos ir atsakomybė:

19.1. EDMIS naudotojams suteikia teisę naudoti IS išteklius ir tvarkyti duomenis jiems priskirtoms funkcijoms atlikti;

19.2. administruoja kompiuterių tinklą sudarančius komponentus (kompiuterius, operacines sistemas, duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, informacijos perdavimo tinklus), nustato pažeidžiamų vietų ir saugos reikalavimų atitiktį;

19.3. valdo informacinės sistemos veiklos ir duomenų mainų integracinius procesus;

19.4. registruoja saugos incidentus ir informuoja apie juos Saugos įgaliotinį, teikia siūlymus dėl minėtų incidentų šalinimo;

19.5. atsako už kompiuterių tinklo ir programinės įrangos funkcionavimą;

19.6. pagal kompetenciją teikia pasiūlymus dėl EDMIS priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

19.7. užtikrina EDMIS duomenų saugumą ir konfidencialumą:

19.7.1. neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;

19.7.2. saugo EDMIS tvarkomų asmens duomenų paslaptį;

19.7.3. neperduoda neįgaliotiems asmenimis slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą EDMIS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su EDMIS tvarkoma elektronine informacija;

19.8. atlieka kitas šiuose saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir kitus EDMIS valdytojo ar Saugos įgaliotinio nurodymus, susijusius su IS sauga.

20. EDMIS naudotojų funkcijos ir atsakomybė:

20.1. vadovaudamiesi EDMIS valdytojo patvirtintais EDMIS nuostatais, šiais saugos nuostatais, EDMIS duomenų teikimo sutartimis, EDMIS naudojimo instrukcijomis ir pareigybių aprašymais, naudoja EDMIS;

20.2. tvarko EDMIS elektroninę informaciją ir naudojasi kitomis EDMIS teikiamomis galimybėmis pagal nustatytą funkcijoms atlikti reikalingą EDMIS prieigos teisių lygmenį, kuris apriboja naudojimosi elektronine informacija apimtį;

20.3. pagal kompetenciją rengia pasiūlymus dėl EDMIS kūrimo, palaikymo, priežiūros ir elektroninės informacijos saugos;

20.4. tvarkydami EDMIS elektroninę informaciją neatskleidžia, neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;

20.5. saugo EDMIS tvarkomų asmens duomenų paslaptį;

20.6. neperduoda neįgaliotiems asmenimis slaptažodžių, naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą EDMIS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su EDMIS tvarkoma elektronine informacija;

20.7. informuoja Saugos įgaliotinį ar administratorius apie elektroninės informacijos saugos incidentus, EDMIS darbo sutrikimus ir teikia pasiūlymus dėl jų pašalinimo;

20.8. vykdo kitas šiuose saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir kitus EDMIS valdytojo, Saugos įgaliotinio ir administratorių nurodymus, susijusius su EDMIS naudojimu ir sauga.

21. Teisės aktai, kuriais vadovaujantis tvarkomi EDMIS duomenys ir užtikrinama jų sauga:

21.1. 2004 m. balandžio 29 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 883/2004 dėl socialinės apsaugos sistemų koordinavimo;

21.2. Lietuvos Respublikos sveikatos draudimo įstatymas (Žin., 1996, Nr. 55-1287; 2002, Nr. 123-5512);

21.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 1996, Nr. 63-1479; 2003, Nr. 15-597; 2000, Nr. 64-1924; 2008, Nr. 22-804);

21.4. Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių įstaigų įstatymas (Žin., 2000, Nr. 10-236; 2005, Nr. 139-5008);

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

21.6. Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 „Dėl elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891; 2008, Nr. 85-3393);

21.7. Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymas Nr. 1V-172 „Dėl Saugos dokumentų turinio gairių patvirtinimo“ (Žin., 2007, Nr. 53-2070);

21.8. Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymas Nr. 1V-384 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimų patvirtinimo ir Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymo Nr. 1V-247 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ pakeitimo“ (Žin., 2008, Nr. 127-4866);

21.9. Lietuvos Respublikos vidaus reikalų ministro 2007 m. liepos 11 d. įsakymas Nr. 1V-247 „Dėl Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (Žin., 2007, Nr. 78-3160);

21.10. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymas Nr. 1T-71(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ (Žin., 2008, Nr. 135-5298);

21.11. Lietuvos standartai LST ISO/IEC 17799:2006 ir LST ISO/IEC 27001:2006 bei Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

21.12. kiti teisės aktai, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, EDMIS valdytojo veikla ir elektroninės informacijos saugos valdymas.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

22. Vadovaujantis Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairių 3.2.1 ir 3.2.7 punktais EDMIS priskiriama antrajai informacinių sistemų kategorijai.

23. EDMIS saugos priemonės parenkamos įvertinus galimus rizikos veiksnius EDMIS duomenų vientisumui ir prieinamumui.

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

24.1. liekamoji rizika turi būti sumažinama iki priimtino lygio;

24.2. informacijos saugos priemonių diegimo kaina turi atitikti saugomos informacijos vertę;

24.3. turi būti įdiegiamos prevencinės, detekcinės ir korekcinės duomenų saugos priemonės.

25. EDMIS kaupiamų duomenų šaltiniai, apdorojimo tvarka ir aprašymas pateikiami EDMIS nuostatuose.

26. Vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugojimo priemonėms, atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, EDMIS duomenys priskiriami antram saugumo lygiui.

27. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos

technologija. Saugumo technika“ grupės standartus, kasmet organizuoja EDMIS rizikos vertinimą. Prireikus Saugos įgaliotinis gali organizuoti neeilinį EDMIS rizikos vertinimą.

28. EDMIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgus į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

28.1. 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);

28.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis EDMIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

28.3. nenugalima jėga.

29. Rizikos įvertinimo ataskaitą tvirtina VLK vadovas. Atsižvelgdamas į rizikos įvertinimo ataskaitą EDMIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

30. Siekiant užtikrinti šiuose nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus turi būti organizuojamas EDMIS informacinių technologijų saugos atitikties vertinimas, kurio metu:

30.1. įvertinama šių nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų ir realios informacijos saugos atitiktis;

30.2. inventorizuojama EDMIS techninė ir programinė įranga;

30.3. tikrinamos Saugos įgaliotinio, EDMIS administratorių bei EDMIS naudotojų, dirbančių VLK, TLK ir SAM, darbo vietose ir visose tarnybinėse stotyse įdiegtos programos ir jų sąranka (būtina patikrinti ne mažiau kaip 10 procentų darbo vietų);

30.4. patikrinama (įvertinama) EDMIS naudotojams suteiktų teisių atitiktis vykdomoms funkcijoms;

30.5. įvertinamas pasirengimas užtikrinti EDMIS veiklos tęstinumą įvykus saugos incidentui (nenumatytai situacijai).

31. Atlikus EDMIS informacinių technologijų saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato EDMIS valdytojas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

32. Saugi prieiga prie EDMIS duomenų yra užtikrinama tokiomis priemonėmis:

32.1. kontroliuojamas patekimas į VLK, TLK ir SAM patalpas, įrengiama signalizacija (nuo įsilaužimo ir gaisro);

32.2. tarnybinių stočių patalpų durys šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis;

32.3. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos dubliuojami ir jų techninė būklė nuolat stebima;

32.4. periodiškai atliekami elektroninės informacijos atkūrimo iš kopijų bandymai;

32.5. programinės įrangos diegimą atlieka tik įgalioti asmenys;

32.6. prieigos prie EDMIS teises suteikia EDMIS administratorius. Pasikeitus EDMIS naudotojo pareigoms ar atliekamoms užduotims, suteikta prieiga turi būti nedelsiant nutraukiama. EDMIS naudotojams suteiktos prieigos teisės periodiškai, bet ne rečiau kaip kartą per metus, turi būti peržiūrimos, siekiant nustatyti ir pašalinti subjektus, kuriems prieigos teisės prie EDMIS turi būti panaikintos arba pakeistos. Už periodinę EDMIS naudotojų teisių peržiūrą atsakingas Saugos įgaliotinis;

32.7. EDMIS naudotojai atpažįstami pagal vartotojų vardus ir slaptažodžius, kurių kontrolę atlieka kompiuterio ir tarnybinės stoties operacinės sistemos;

32.8. prisijungimo prie sistemos slaptažodis keičiamas ne rečiau kaip kas 3 mėnesius;

32.9. slaptažodį sudaro 8 ir daugiau simbolių;

32.10. keičiant slaptažodį, IS neleidžia nustatyti slaptažodžio iš 6 paskutinių slaptažodžių;

32.11. nustatytas ne didesnis kaip 3 leistinų nevykusių bandymų prisijungti prie EDMIS skaičius;

32.12. prieiga prie duomenų gali būti suteikta tik tam asmeniui, kuriam tie duomenys yra reikalingi jo funkcijoms vykdyti;

32.13. su sistemos duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti yra suteiktos teisės;

32.14. asmenų, kuriems suteikta teisė tvarkyti duomenis, veiksmai yra registruojami, audituojami ir saugomi ne trumpiau kaip 1 metus;

32.15. ne rečiau kaip vieną kartą per mėnesį peržiūrimas naudotojų prisijungimų prie duomenų bazių elektroninis žurnalas ir parengiamas peržiūros ataskaitos;

32.16. prieiga prie kompiuterių ir tarnybinių stočių operacinių sistemų valdymo ir konfigūravimo leidžiama tik administratoriams.

33. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami.

34. Informacinė sistema pasiekiama visą parą.

35. Išorinės duomenų laikmenos, kuriose saugomi gaunami ir teikiami asmens duomenys, registruojamos ir kontroliuojamas jų panaudojimas, ištrinant asmens duomenis po jų panaudojimo perkeliant į duomenų bazes.

36. Kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.

37. Kompiuterinės įrangos gedimai ir avarinio asmens duomenų atkūrimo veiksmai registruojami žurnale.

38. Antivirusinė programa yra valdoma iš pagrindinės tarnybinės stoties. Naudotojų kompiuterių antivirusinės programos turi būti kasdien atnaujinamos iš pagrindinės tarnybinės stoties.

39. EDMIS naudotojams draudžiama diegti bet kokią programinę įrangą. Programinę įrangą, reikalingą naudotojo funkcijoms vykdyti, diegia ir prižiūri administratoriai.

40. Draudžiama naudoti programinę įrangą, nesusijusią su įstaigos veikla.

41. Neteisėtų programų diegimo paieška (apeinant operacinės sistemos apsaugos mechanizmus) atliekama bent kartą per 6 mėnesius.

42. Programinės įrangos testavimas atliekamas naudojant atskirą tam skirtą testavimo aplinką.

43. EDMIS programinis kodas turi būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

44. Naudojami tarnybinės stoties operacinės sistemos metodai, leidžiantys vienareikšmiškai atpažinti kompiuterių tinklui priklausančius kompiuterius.

45. Draudžiama prieiga neatpažintiems vartotojams prisijungti prie kompiuterių tinklo iš kompiuterio, nepriklausančio šiam tinklui.

46. Tarnybinių stočių patalpose įrengta oro kondicionavimo įranga ir drėgmės kontrolės įranga.

47. Patekimas prie darbo vietų kontroliuojamas.

48. Kiekvienas kompiuteris priskiriamas atsakingam naudotojui.

49. Draudžiama keisti kabinetuose kompiuterių išdėstymo vietas be administratoriaus leidimo.

50. Kompiuteriai naudojami tik tarnybinėms funkcijoms vykdyti.

51. Nešiojamieji kompiuteriai ne VLK, TLK ir SAM patalpose gali būti naudojami tik tarnybinėms funkcijoms vykdyti.

52. Nešiojamieji kompiuteriai, jei juose yra prisijungimo prie EDMIS duomenų galimybė nesant savos darbo vietos patalpose, iš VLK, TLK ir SAM patalpų gali būti išnešami tik pagal VLK, TLK ar SAM vadovo ar jo įgalioto asmens išrašytą leidimą, raštu patvirtinantį naudotojo asmeninę atsakomybę už informacijos saugą ir nurodantį kompiuterio naudojimo tikslą ir laikotarpį, kuriam kompiuteris išnešamas.

53. Nešiojamuosiuose kompiuteriuose, išnešamuose iš VLK, TLK ir SAM patalpų, esantys duomenys šifruojami priemonėmis, atitinkančiomis duomenų tvarkymo keliamą riziką.

54. Iš nutolusių darbo vietų jungiamasi per IP VPN (virtualus privatus tinklas).

55. EDMIS duomenys perduodami automatiniu būdu TCP/IP protokolu realiu laiku arba asinchroniniu režimu pagal EDMIS duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka.

56. Už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų identifikavimą, suformulavimą ir įgyvendinimo organizavimą atsakingas Saugos įgaliotinis.

57. EDMIS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijos tinklų naudojant užkardą.

58. Konfigūruojant EDMIS elektroninės informacijos perdavimo tinklo užkardas turi būti naudojami tik organizacijos veiklai būtini tinklo protokolai ir užkardų prievadai.

59. Saugos įgaliotinis organizuoja EDMIS serverių srities tinklo užkardų administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią užkardų konfigūraciją.

60. Užkardų konfigūracija peržiūrima ne rečiau kaip kartą per metus. Peržiūrą inicijuoja Saugos įgaliotinis.

61. EDMIS tarnybinėse stotyse esančios informacijos atsarginės duomenų kopijos turi būti daromos kiekvieną darbo dieną.

62. Atkurti informaciją iš atsarginių duomenų kopijų turi būti įmanoma per 1 darbo dieną. Atsarginės duomenų kopijos turi būti saugomos ne mažiau kaip 5 dienas.

63. Atsarginės duomenų kopijos saugomos kitoje patalpoje nei yra įrenginys, kurio informacija buvo nukopijuota.

64. Už atsarginių EDMIS duomenų kopijų darymo ir atkūrimo ir už EDMIS taikomosios programinės įrangos kopijų darymo organizavimą ir peržiūrą yra atsakingas Saugos įgaliotinis.

IV. REIKALAVIMAI PERSONALUI

65. Tvarkyti EDMIS duomenis gali asmenys, susipažinę su EDMIS nuostatais, informacinių sistemų saugos politiką reglamentuojančiais teisės aktais.

66. Saugos įgaliotinis turi turėti informacinių technologijų specialisto kvalifikaciją, išmanyti informacinių sistemų administravimą, gerai išmanyti elektroninės informacijos saugos principus bei saugos užtikrinimo metodus, savo darbe vadovautis Saugos nuostatais, Informacinių technologijų saugos atitikties vertinimo metodika, kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą, standartais ir kitais dokumentais.

67. EDMIS administratoriai turi išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais, taip pat kitomis vidaus ir darbo taisyklėmis.

68. EDMIS naudotojai turi būti įgiję darbo kompiuteriu įgūdžių, mokėti tvarkyti EDMIS duomenis EDMIS nuostatuose nurodyta tvarka, išmanyti informacinių sistemų saugos politiką reglamentuojančius teisės aktus.

69. EDMIS naudotojai turi dirbti vadovaudamiesi sistemos techninėje dokumentacijoje nustatyta tvarka. EDMIS naudotojai privalo rūpintis tvarkomų duomenų saugumu. Pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, EDMIS naudotojai privalo nedelsdami

apie tai pranešti Saugos įgaliotiniui.

70. Saugos įgaliotinis periodiškai inicijuoja informacinės sistemos naudotojų mokymą duomenų saugos klausimais, įvairiais būdais informuoja juos apie duomenų saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujai priimtiems darbuotojams, pagal poreikį organizuojami susitikimai su EDMIS tvarkytojų atsakingais asmenimis).

71. EDMIS naudotojų mokymus Saugos įgaliotinis, EDMIS administratorius arba mokymų paslaugų teikėjas, su kuriuo VLK pasirašo paslaugų sutartį, vykdo ne rečiau nei kartą per 3 metus.

72. Esant elektroninės informacijos saugos incidentui, nenumatytai situacijai, Saugos įgaliotinio, administratorių ir naudotojų veiksmus reglamentuoja VLK vadovo įsakymu tvirtinamas EDMIS veiklos tęstinumo valdymo planas.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

73. Naudotojų supažindinimą pasirašytinai su šiais nuostatais ir kitais saugos politiką reglamentuojančiais dokumentais organizuoja Saugos įgaliotinis ir EDMIS tvarkytojų vadovai.

74. Saugos įgaliotinis reguliariai įvairiais būdais informuoja naudotojus apie informacijos saugos problematiką.

VI. BAIGIAMOSIOS NUOSTATOS

75. Saugos nuostatai ir kiti saugos politiką reglamentuojantys teisės aktai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus.

76. EDMIS tvarkytojai turi įgyvendinti Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose saugų EDMIS duomenų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

77. Saugos įgaliotinis ir EDMIS administratoriai raštu įsipareigoja nepažeisti Saugos nuostatų ir kitų teisės aktų, reglamentuojančių EDMIS duomenų saugų tvarkymą.

78. Saugos įgaliotinis, EDMIS administratoriai ir informacinės sistemos naudotojai, pažeidę Saugos nuostatų, kitų teisės aktų, reglamentuojančių EDMIS duomenų saugų tvarkymą, reikalavimus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.

_____