Patvirtinta
UAB Riešės šeimos klinika
Direktorės įsakymu
2017 m. 08 21 d. įsakymu Nr. 17/08/21-1

INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS

BENDROSIOS NUOSTATOS

1. UAB Riešės šeimos klinikos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Informacinės sistemos POLIS (toliau POLIS IS) duomenų saugą ir apibrėžia POLIS IS saugos politiką (toliau – saugos politika), kuri įgyvendinama vadovaujantis šiais teisės aktais (toliau – saugos politiką įgyvendinantys teisės aktai):

1.1. POLIS IS saugaus elektroninės informacijos tvarkymo taisyklėmis;

1.2. POLIS IS naudotojų administravimo taisyklėmis;

1.3. POLIS IS veiklos tęstinumo valdymo planu.

2. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos vyriausybės 2013 m. liepos 24 d. nutarime Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), POLIS IS nuostatuose ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014 vartojamas sąvokas.

3. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys – paciento asmens ir ypatingų sveikatos duomenų, susijusių su elektronine medicinine istorija (toliau – EMI), saugus ir teisėtas tvarkymas, prieinamumo, vientisumo ir konfidencialumo užtikrinimas.

4. POLIS IS duomenų saugos tikslai:

4.1. informacijos patikimumo, vientisumo, konfidencialumo, prieinamumo ir saugumo užtikrinimas;

4.2. kompiuterizuotų darbo vietų tinkamo saugumo lygio įdiegimas ir palaikymas;

4.3. nuolatinis vietinio kompiuterių tinklo funkcionavimo užtikrinimas bei saugumo stebėsena;

4.4. tinkamo kompiuterinės, programinės ir tinklo įrangos funkcionavimo ir saugumo užtikrinimas.

5. EMI, informacinės sistemos duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, organizacinės, fizinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos lygio kėlimo, saugos priemonių projektavimo ir diegimo principus.

6. Informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1. POLIS IS perduodamų duomenų konfidencialumo užtikrinimas;

6.2. POLIS IS perduodamų duomenų vientisumo užtikrinimas;

6.3. POLIS IS duomenų prieinamumo užtikrinimas;

6.4. POLIS IS veiklos tęstinumo užtikrinimas.

7. Saugos nuostatų reikalavimai taikomi POLIS IS valdytojui, POLIS IS tvarkytojams, POLIS IS saugos įgaliotiniams, POLIS IS administratoriams ir POLIS IS naudotojams.

8. POLIS IS valdytojas ir tvarkytojas yra UAB Vita Longa klinika, adresas A. Stulginskio g. 67,

Kaunas.

9. POLIS IS valdytojo ir tvarkytojo funkcijos ir atsakomybė:

9.1. organizuoja POLIS IS veiklą ir jai vadovauja;

9.2. tvirtina dokumentus, susijusius su POLIS IS sauga;

9.3. priima sprendimą dėl POLIS IS informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

9.4. skiria POLIS IS vyriausiąjį saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti saugos dokumentų įgyvendinimą POLIS IS;

9.5. atsako už informacijos tvarkymo POLIS IS teisėtumą ir duomenų saugą.

9.6. skiria POLIS IS administratorių (-ius) ir paveda jam (-iems) užtikrinti POLIS IS kompiuterinės įrangos ir POLIS IS naudotojų kompiuterizuotų darbo vietų saugų funkcionavimą, administruoti POLIS IS duomenų bazę saugos dokumentų ir kitų teisės aktų nustatyta tvarka;

9.7. atlieka POLIS IS duomenų bazių priežiūrą;

9.8. užtikrina POLIS IS sąveiką su kitomis informacinėmis sistemomis;

9.9. atlieka POLIS IS duomenų bazių techninę priežiūrą ir užtikrina nepertraukiamą POLIS IS veikimą;

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

9.11. atlieka kitas POLIS IS nuostatų, Saugos nuostatų, Saugos reikalavimų ir kitų teisės aktų nustatytas funkcijas.

10. POLIS IS saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą POLIS IS, atlieka šias funkcijas:

10.1. teikia POLIS IS valdytojo vadovui pasiūlymus dėl:

10.1.1. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.2. POLIS IS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

10.2. teikia POLIS IS vadovui siūlymus dėl POLIS IS administratoriaus (-ių) paskyrimo;

10.3. įgyvendina POLIS IS duomenų saugą, vadovaudamasis Saugos reikalavimais;

10.4. koordinuoja elektroninės informacijos saugos incidentų POLIS IS tyrimą;

10.5. pagal kompetenciją teikia POLIS IS administratoriui (-iams) privalomus vykdyti nurodymus ir pavedimus, koordinuoja POLIS IS administratoriaus (-ių) veiklą;

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

10.7. atsako už POLIS IS saugos dokumentų reikalavimų vykdymą;

10.8. periodiškai organizuoja POLIS IS naudotojų mokymą duomenų saugos klausimais, reguliariai jiems primena saugos problemas (elektroniniu paštu, parengia atmintines naujai priimtiems darbuotojams ir pan.);

10.9. kasmet organizuoja POLIS IS rizikos įvertinimą;

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

11. POLIS IS administratorius atlieka šias funkcijas:

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

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

11.3. rengia pasiūlymus POLIS IS tvarkytojui dėl POLIS IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

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

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

13. POLIS IS sistemos duomenys tvarkomi ir POLIS IS duomenų sauga užtikrinama, vadovaujantis:

13.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

13.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

13.3. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu;

13.4. Lietuvos Respublikos sveikatos sistemos įstatymu;

13.5. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

13.6. Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymu;

13.7. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

13.8. Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymas Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

13.9. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymu Nr. 1T-74(1.12.E) „Dėl Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. Įsakymo Nr. 1T-12(1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ pakeitimo;

13.10. Lietuvos standartais LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, reglamentuojančiais saugų duomenų tvarkymą;

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

II SKYRIUS

POLIS IS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.3. papunkčiu, POLIS IS tvarkoma elektroninė informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai. Elektroninės informacijos priskyrimo žinybinės svarbos kategorijai kriterijai:

14.1. gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų teisėtiems interesams;

14.2. gali turėti neigiamų padarinių institucijos veiklai;

14.3. gali sukelti kitų neigiamų padarinių institucijai.

15. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų

klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.3 papunkčiu, POLIS IS priskiriama trečiosios kategorijos informacinėms sistemoms – POLIS IS tvarkoma žinybinės svarbos elektroninė informacija. Atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką bei vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymo Nr. 1T-74(1.12E), 11.3 papunkčiu, POLIS IS priskiriama trečiajam automatiniu būdu tvarkomų asmens duomenų saugumo lygiui.

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

17. POLIS IS kaupiamų ir apdorojamų duomenų rinkimo tvarka, kriterijai bei sąrašas pateikiami POLIS IS nuostatuose. POLIS IS vyriausiasis saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja POLIS IS rizikos vertinimą. Prireikus POLIS IS saugos įgaliotinis gali organizuoti neeilinį POLIS IS rizikos vertinimą. POLIS IS saugos įgaliotinį paskyrusio valdytojo vadovo rašytiniu pavedimu POLIS IS rizikos vertinimą gali atlikti pats POLIS IS saugos įgaliotinis.

18. POLIS IS rizikos vertinimo metu atliekamos šios veiklos:

18.1. POLIS IS sudarančių išteklių inventorizacija;

18.2. rizikos veiksnių įtakos POLIS IS vertinimas;

18.3. liekamosios rizikos vertinimas.

19. POLIS IS valdytojas POLIS IS rizikos vertinimą gali pavesti atlikti trečiajai šaliai.

20. POLIS IS rizikos veiksnių įvertinimas atliekamas kokybiniu rizikos vertinimo metodu ir pateikimas Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausieji rizikos veiksniai, kurie gali pažeisti POLIS IS duomenų ir parengtos pagal juos informacijos saugą, yra:

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, neteisingas veikimas ir kita);

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

20.3. nenugalima jėga (force majeure).

21. Atsižvelgdamas į rizikos vertinimo ataskaitą, POLIS IS valdytojas, prireikus, tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis POLIS IS rizikos valdymo priemonėms įgyvendinti.

22. Pagrindiniai POLIS IS elektroninės informacijos saugos priemonių parinkimo principai yra šie:

22.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

22.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

22.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

23. Įvykus POLIS IS elektroninės informacijos saugos incidentui, nenumatytai situacijai, POLIS IS saugos įgaliotinių, POLIS IS administratorių ir POLIS IS naudotojų veiksmus reglamentuoja POLIS IS veiklos tęstinumo valdymo planas.

24. Siekiant užtikrinti Saugos nuostatuose ir Saugos politiką įgyvendinančiuose teisės aktuose išdėstytų Saugos nuostatų įgyvendinimo kontrolę, POLIS IS saugos įgaliotinis kasmet, iki gruodžio 30 d., organizuoja POLIS IS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

24.1. įvertinama informacijos saugos atitiktis saugos dokumentams;

24.2. inventorizuojama POLIS IS techninė ir programinė įranga;

24.3. patikrinama ne mažiau kaip 10 proc. atsitiktinai parinktų POLIS IS naudotojų kompiuterizuotų darbo vietų, POLIS IS tarnybinėse stotyse įdiegtos programos ir jų sąranka;

24.4. patikrinama (įvertinama) POLIS IS naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

24.5. įvertinamas pasirengimas užtikrinti POLIS IS veiklos tęstinumą įvykus POLIS IS elektroninės informacijos saugos incidentui.

25. Atlikus POLIS IS informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus POLIS IS valdytojo vadovas.

26. Neeilinis POLIS IS rizikos vertinimas turi būti atliekamas:

26.1. įvykus pokyčiams POLIS IS techninėje ar programinėje įrangoje, kurie galėtų turėti įtakos POLIS IS veikimui;

26.2. atsiradus naujų tendencijų informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė POLIS IS techninei, programinei įrangai ar POLIS IS laikomiems duomenims;

26.3. po saugos incidento, kurio metu buvo sutrikdyta POLIS IS veikla, sugadinti ar prarasti POLIS IS duomenys.

27. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas POLIS IS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS

ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. POLIS IS naudotojų darbo vietose veikia programinė įranga, skirta kovai su kenksminga programine įranga, automatiškai atnaujinama ne rečiau kaip kas septynias paras.

29. Programinės įrangos, ribojančios programinės įrangos, nesusijusios su POLIS IS veikla ar POLIS IS naudotojų funkcijomis, naudojimo reikalavimai:

29.1. POLIS IS naudotojams leidžiama naudoti tik legalią programinę įrangą;

29.2. periodiškai, ne rečiau kaip kartą per 6 mėnesius, turi būti tikrinama, ar nenaudojama POLIS IS naudotojų darbo vietose nelegali programinė įranga. Rasta nelegali programinė įranga turi būti nedelsiant pašalinta.

30. POLIS IS objektų duomenims saugiai rinkti, apdoroti, kaupti, saugoti, naikinti ir teikti POLIS IS turi būti taikomos šios programinės ir techninės įrangos naudojimą ribojančios pagrindinės priemonės:

30.1. POLIS IS naudotojams prieiga prie POLIS IS duomenų suteikiama tik užsiregistravus (įvedus informacinės sistemos naudotojo vardą ir slaptažodį) arba naudojant elektroninio parašo kvalifikuotą sertifikatą. POLIS IS administratoriai savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni (nei POLIS IS naudotojų slaptažodžiams) reikalavimai arba naudojant elektroninio parašo kvalifikuotą sertifikatą;

30.2. POLIS IS naudotojų prieigos valdymas apibrėžtas POLIS IS naudotojų administravimo taisyklėse;

30.3. POLIS IS naudotojas, baigęs darbą, turi imtis priemonių, kad su POLIS IS elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo POLIS IS, įjungti ekrano užsklandą su slaptažodžiu, dokumentus padėti į pašaliniams asmenims neprieinamą vietą;

30.4. naudojamos ugniasienės;

30.5. tarnybinėse stotyse ir darbo vietose naudojama antivirusinė programinė įranga, kurios maksimalus neatsinaujinimo terminas yra 30 (trisdešimt) kalendorinių dienų;

30.6. programinėmis priemonėmis registruojamos POLIS IS esančios informacijos užklausos, pakeitimai, juos atlikusio POLIS IS naudotojo tapatybė ir pakeitimų atlikimo laikas.

31. Pagrindiniai POLIS IS duomenų bazės atsarginių kopijų darymo ir atkūrimo reikalavimai:

31.1. duomenų saugai užtikrinti daromos pagrindinės POLIS IS duomenų bazės atsarginės duomenų kopijos;

31.2. POLIS IS duomenų bazės atsarginės kopijos daromos diskinėse laikmenose;

31.3. atsarginės POLIS IS duomenų bazės kopijos saugomos kitose patalpose;

31.4. POLIS IS duomenų bazės atsarginės kopijos diskinėse laikmenose daromos reguliariai, kiekvieną darbo dieną;

31.5. sukurtai POLIS IS duomenų bazės atsarginei kopijai nurodoma kopijavimo data;

31.6. kiekvienos savaitės paskutinei POLIS IS duomenų bazės atsarginei kopijai papildomai nurodoma, kad tai yra savaitinė kopija;

31.7. kiekvieno mėnesio paskutinei POLIS IS duomenų bazės atsarginei kopijai papildomai nurodoma, kad tai yra mėnesinė kopija;

31.8. kiekvienų metų paskutinei POLIS IS duomenų bazės atsarginei kopijai papildomai nurodoma, kad tai yra metinė kopija;

31.9. POLIS IS duomenų bazės atsargines dokumentų kopijas turi teisę daryti tik POLIS IS administratorius, kurio pareigybės aprašyme numatyta ši funkcija;

31.10. darant (padarius) POLIS IS duomenų bazės atsargines kopijas, būtina užtikrinti kopijų kokybę;

31.11. POLIS IS duomenų bazės atsarginės kopijos saugomos specializuotos tarnybinės stoties diskinėse laikmenose;

31.12. POLIS IS duomenų bazės atsarginės metinės kopijos saugomos 10 metų nuo jų sukūrimo dienos. POLIS IS duomenų bazės atsarginės mėnesinės kopijos saugomos 1 metus nuo jų sukūrimo dienos. POLIS IS duomenų bazės atsarginės savaitinės kopijos saugomos 1 mėnesį nuo jų sukūrimo dienos;

31.13. POLIS IS duomenų atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik POLIS IS administratorius;

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

32. Nešiojamuose kompiuteriuose POLIS IS programinė įranga nebus diegiama ir duomenys lokaliai nebus saugomi, o POLIS IS bus naudojamasi per interneto naršyklę.

33. POLIS IS telekomunikacinio tinklo apsaugos priemonės:

33.1. tinklo segmentavimas;

33.2. prieigos kontrolės sąrašai (ACL);

33.3. „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;

33.4. tinklo adresų transliavimas (NAT/PAT);

34. pagrindinė POLIS IS duomenų pateikimo prieiga yra duomenų perdavimas duomenų

perdavimo kanalu, panaudojant saugų HTTPS (angl. *Hypertext Transfer Protocol Secure*) duomenų perdavimo protokolą. POLIS IS naudotojai identifikuojami ir jiems suteikiamos teisės pagal jam suteiktą naudotojo vardą ir slaptažodį.

35. POLIS IS duomenys, perduodami ne per POLIS IS tvarkytojui priklausančias duomenų perdavimo linijas, privalo būti šifruojami.

36. Saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

37. POLIS IS duomenų gavimo automatiniu būdu iš kitų informacinių sistemų tvarka nustatoma duomenų teikimo sutartyse.

IV SKYRIUS

REIKALAVIMAI PERSONALUI

38. POLIS IS saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Saugos dokumentais, Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais POLIS 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.

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

40. POLIS 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.

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

42. POLIS IS naudotojai, pastebėję saugos dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai POLIS IS administratoriams arba POLIS IS saugos įgaliotiniui.

43. POLIS IS administratorius apie Saugos nuostatų 422 punkte nurodytus pažeidimus informuoja POLIS IS saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią POLIS IS saugą (jos konfidencialumą, vientisumą ar prieinamumą), POLIS IS įgaliotinis apie tai turi pranešti kompetentingoms institucijoms.

44. POLIS IS naudotojų informacijos saugos mokymai ir žinių atnaujinimas atliekamas kasmet. Už tai atsakingas POLIS IS saugos įgaliotinis.

45. POLIS IS saugos įgaliotinis periodiškai įvairiais būdais informuoja juos apie informacijos saugą (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems

darbuotojams ir panašiai).

V SKYRIUS

POLIS IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

46. Tvarkyti POLIS IS duomenis gali tik įgalioti POLIS IS naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

47. Už POLIS IS naudotojų supažindinimą su saugos dokumentais, kitais teisės aktais, nurodytais Saugos nuostatų 13 punkte, kuriais vadovaujamasi tvarkant POLIS IS elektroninę informaciją, užtikrinant jos saugumą, atsakomybę už saugos dokumentų nuostatų pažeidimus, informacijos saugos mokymą ir žinių atnaujinimą atsako POLIS IS saugos įgaliotinis.

48. Tvarkyti POLIS IS duomenis gali tik įgalioti POLIS IS naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. POLIS IS saugos įgaliotinis raštu informuoja POLIS IS naudotojus apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios.

VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

49. POLIS IS valdytojas ir tvarkytojas, POLIS IS Saugos įgaliotinis, POLIS IS administratoriai ir POLIS IS naudotojai, pažeidę šių Saugos nuostatų ir kitų saugų informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____