LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2016 M. KOVO 22 D. ĮSAKYMO NR. V-372 „DĖL VISUOMENĖS SVEIKATOS PRIEŽIŪROS SPECIALISTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2018 m. rugsėjo 11 d. Nr. V-1005
Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. kovo 22 d. įsakymą Nr. V-372 „Dėl Visuomenės sveikatos priežiūros specialistų registro duomenų saugos nuostatų patvirtinimo“:

1. Pakeičiu preambulę ir ją išdėstau taip:

„Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 5 ir 7 punktais:“.

2. Pakeičiu suderinimo žymą ir ją išdėstau taip:

„SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugpjūčio 28 d. raštu Nr. (4.2) 6K-519“.

3. Pakeičiu nurodytu įsakymu patvirtintus Visuomenės sveikatos priežiūros specialistų registro duomenų saugos nuostatus ir juos išdėstau nauja redakcija (pridedama).

Sveikatos apsaugos ministras Aurelijus Veryga

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2016 m. kovo 22 d. įsakymu Nr. V-372
(Lietuvos Respublikos sveikatos apsaugos
ministro 2018 m. rugsėjo 11 d.
įsakymo Nr. V-1005 redakcija)

VISUOMENĖS SVEIKATOS PRIEŽIŪROS SPECIALISTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Visuomenės sveikatos priežiūros specialistų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Visuomenės sveikatos priežiūros specialistų registro (toliau – Registras) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – Saugos politika), kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti Registro elektroninę informaciją, kad ji būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto tvarkymo.

2. Saugos politika įgyvendinama taip pat vadovaujantis Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. liepos 12 d. įsakymu Nr. V-926 „Dėl Visuomenės sveikatos priežiūros specialistų registro naudotojų administravimo taisyklių, Visuomenės sveikatos priežiūros specialistų registro saugaus elektroninės informacijos tvarkymo taisyklių ir Visuomenės sveikatos priežiūros specialistų registro veiklos tęstinumo valdymo plano patvirtinimo“.

3. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka teisės aktuose, nurodytuose šių Saugos nuostatų 16 punkte, vartojamas sąvokas.

4. Šiais Saugos nuostatais turi vadovautis Registro valdytojas, Registro tvarkytojai, Registro duomenų valdymo įgaliotinis, Registro saugos įgaliotinis (toliau – Saugos įgaliotinis), Registro kompetentingas asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – Kibernetinio saugumo vadovas), Registro administratorius (toliau – Administratorius), Registro naudotojai (toliau – Naudotojai), paslaugų, susijusių su Registro veikimu, teikėjai.

5. Registro duomenų saugos ir kibernetinio saugumo (toliau – Registro duomenų sauga) tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti Registro duomenis, užtikrinant duomenų konfidencialumą, vientisumą ir prieinamumą.

6. Registro duomenų saugos užtikrinimo prioritetinės kryptys:

6.1. Registro duomenų konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

6.2. administracinių saugaus darbo su duomenimis priemonių įgyvendinimas ir kontrolė;

6.3. Registro duomenims tvarkyti naudojamos techninės ir programinės įrangos kontrolė.

7. Registro valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija (toliau – Ministerija), buveinės adresas: Vilnius, Vilniaus g. 33.

8. Registro tvarkytojai yra Higienos institutas (toliau – Institutas) ir Lietuvos nacionalinės sveikatos sistemos visuomenės sveikatos priežiūros įstaigos (toliau – Įstaigos), pavaldžios Registro valdytojui. Instituto buveines adresas: Vilnius, Didžioji g. 22. Įstaigų pavadinimai, jų buveinių adresai nurodyti Ministerijos tinklalapyje www.sam.lt. Registro tvarkytojai yra ir asmens duomenų tvarkytojai.

9. Registro valdytojas atlieka šias funkcijas:

9.1. tvirtina Registro saugos politiką įgyvendinančius dokumentus (toliau – Saugos dokumentai): Saugos nuostatus, Visuomenės sveikatos priežiūros specialistų registro naudotojų administravimo taisykles, Visuomenės sveikatos priežiūros specialistų registro saugaus elektroninės informacijos tvarkymo taisykles ir Visuomenės sveikatos priežiūros specialistų registro veiklos tęstinumo valdymo planą, kitus dokumentus, susijusius su Registro duomenų sauga;

9.2. priima sprendimus dėl techninių ir programinių priemonių, būtinų Registro duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.3. nagrinėja Registro tvarkytojų pasiūlymus dėl registro duomenų saugos priemonių tobulinimo ir priima sprendimus dėl jų finansavimo;

9.4. organizuoja Registro veiklą ir jai vadovauja;

9.5. paveda Registro tvarkytojui Institutui skirti Registro duomenų valdymo įgaliotinį, Saugos įgaliotinį ir Administratorių;

9.6. prižiūri saugos reikalavimų įgyvendinimą;

9.7. priima sprendimus dėl Registro informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

9.8. kontroliuoja, kad Registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, Saugos dokumentais ir kitais teisės aktais;

9.9. atlieka kitas Saugos nuostatų 16 punkte nurodytuose teisės aktuose valdytojui priskirtas funkcijas, susijusias su Registro duomenų sauga.

10. Registro tvarkytojo Instituto funkcijos:

10.1. Registro valdytojui pavedus skiria Saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti saugos reikalavimų įgyvendinimą;

10.2. Registro valdytojo pavedimu skiria Administratorių ir paveda prižiūrėti Registrą ir jo infrastruktūrą, užtikrinant jo veikimą ir Registro duomenų saugą;

10.3. skiria Kibernetinio saugumo vadovą;

10.4. įgyvendina tinkamas organizacines ir technines priemones, skirtas duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

10.5. užtikrina, kad Naudotojai, turintys teisę naudotis Registro duomenimis numatytoms funkcijoms atlikti, laikytųsi reikalavimų, nustatytų Saugos nuostatuose ir kituose Saugos politiką įgyvendinančiuose teisės aktuose;

10.6. organizuoja techninių, programinių priemonių, skirtų Registrui eksploatuoti, prižiūrėti ir plėtoti, įsigijimą, jų įdiegimą ir modernizavimą, registro techninės, programinės įrangos priežiūrą ir tobulinimą;

10.7. pagal kompetenciją atsako už Registro duomenų tvarkymo teisėtumą ir duomenų saugumą bei Registro saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir šiems Saugos nuostatams;

10.8. organizuoja Saugos dokumentų peržiūrėjimą ne rečiau kaip kartą per metus, esant poreikiui juos keičia;

10.9. atlieka kitas Saugos nuostatų 16 punkte nurodytuose teisės aktuose nustatytas funkcijas, susijusias su Registro duomenų sauga.

11. Registro tvarkytojos Įstaigos:

11.1. įgyvendina Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Registro duomenų saugų tvarkymą, nustatytas organizacines, technines ir kitas priemones;

11.2. užtikrina, kad jų įstaigose dirbantys Registro naudotojai laikytųsi Saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nurodytų reikalavimų.

12. Saugos įgaliotinio funkcijos:

12.1. teikia Registro valdytojui ar tvarkytojui Institutui siūlymus dėl Administratoriaus skyrimo, Saugos dokumentų priėmimo, keitimo ar panaikinimo, saugos reikalavimų atitikties vertinimo atlikimo;

12.2. teikia Administratoriui privalomus vykdyti nurodymus ir pavedimus;

12.3. konsultuoja Naudotojus saugaus duomenų tvarkymo klausimais;

12.4. inicijuoja Administratoriaus ir Naudotojų mokymą duomenų saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

12.5. organizuoja kasmetinį Registro rizikos vertinimą;

12.6. atsako už duomenų saugumo politikos įgyvendinimą ir saugos dokumentų reikalavimų vykdymą;

12.7. atlieka kitas Saugos dokumentuose ir kituose Saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

13. Administratoriaus funkcijos:

13.1. suteikia Naudotojams prieigos teisę naudotis Registro duomenimis, reikalingais jiems priskirtoms funkcijoms atlikti; registruoja kitų Registro tvarkytojų – Įstaigų – Naudotojus, gavęs Įstaigos vadovo raštišką prašymą;

13.2. registruoja elektroninės informacijos saugos incidentus ir koordinuoja jų tyrimą;

13.3. informuoja Saugos įgaliotinį apie elektroninės informacijos saugos incidentus;

13.4. teikia siūlymus dėl duomenų saugos organizavimo;

13.5. atsako, kad tvarkant Registrą nebūtų pažeisti Saugos nuostatų reikalavimai;

13.6. organizuoja Registro kompiuterinės ir programinės įrangos administravimą ir priežiūrą, siekdamas užtikrinti kokybišką ir patikimą jos veikimą;

13.7. atsako už Registro duomenų bazės duomenų atsarginių kopijų darymą ir saugojimą;

13.8. atlieka kitas Saugos dokumentuose ir kituose Saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

14. Kibernetinio saugumo vadovas vykdo Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m.

balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas) ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose jam priskirtas funkcijas.

15. Naudotojų funkcijos:

15.1. informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojasi ir tvarko elektroninę informaciją;

15.2. informuoja Saugos įgaliotinį apie elektroninės informacijos saugos incidentus, o Administratorių – apie Registro darbo sutrikimus;

15.3. vykdo kitas Saugos nuostatuose ir Saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su Registro naudojimu ir duomenų sauga;

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

16. Registro duomenų sauga užtikrinama vadovaujantis:

16.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

16.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

16.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

16.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);

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

16.6. Kibernetinio saugumo reikalavimų aprašu;

16.7. Visuomenės sveikatos priežiūros specialistų registro nuostatais, patvirtintais Lietuvos Respublikos Vyriausybės 2015 m. lapkričio 18 d. nutarimu Nr. 1207 „Dėl žinybinio Visuomenės sveikatos priežiūros specialistų registro įsteigimo, jo nuostatų patvirtinimo ir veiklos pradžios nustatymo“;

16.8. kitais teisės aktais, reglamentuojančiais elektroninės informacijos Saugos politiką ir Registro duomenų tvarkymo teisėtumą bei duomenų saugumo valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios

valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas) 9.1 ir 9.2 papunkčiais, Registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai.

18. Vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčio nuostatomis, atsižvelgiant į Registre apdorojamos elektroninės informacijos svarbos kategoriją, Registras priskiriamas trečiajai kategorijai.

19. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius Registro duomenų vientisumui, konfidencialumui ir prieinamumui. Saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos įvertinimą, kuris apima ir grėsmių bei pažeidžiamumų, galinčių turėti įtakos Registro kibernetiniam saugumui, įvertinimą. Minėtą rizikos įvertinimą gali atlikti ir pats Saugos įgaliotinis. Saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

20. Registro rizikos įvertinimas pateikiamas rizikos įvertinimo ataskaitoje, kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Šioje ataskaitoje išdėstomos pagrindinės Registro rizikos valdymo priemonės. Registro rizikos įvertinimo ataskaitą kasmet iki gruodžio 20 d. parengia Saugos įgaliotinis ir ne vėliau kaip per 2 darbo dienas nuo jos parengimo dienos pateikia Registro tvarkytojo vadovui, kuris ne vėliau kaip per 3 darbo dienas nuo Registro rizikos įvertinimo ataskaitos gavimo dienos ją patvirtina.

21. Pagrindiniai rizikos veiksniai, galintys turėti įtakos Registro duomenų saugumui, yra šie:

21.1. 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);

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

21.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos *(force majeure)* aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos *(force majeure)* aplinkybėms taisyklių patvirtinimo“, 3 punkte.

22. Saugos užtikrinimo priemonės parenkamos siekiant užtikrinti Registro veiklos tęstinumą patiriant kuo mažiau išlaidų ir užtikrinant saugų Registro darbą.

23. Saugos įgaliotinis ne vėliau kaip per 3 darbo dienas nuo Registro rizikos įvertinimo atlikimo dienos parengia Registro rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti, nurodomi atsakingi vykdytojai, priemonių įgyvendinimo terminai. Saugos įgaliotinis Registro rizikos įvertinimo ir rizikos valdymo priemonių planą ne vėliau kaip per 2 darbo dienas nuo jo parengimo dienos pateikia Registro tvarkytojo vadovui, kuris ne

vėliau kaip per 3 darbo dienas nuo Registro rizikos įvertinimo ir rizikos valdymo priemonių plano gavimo dienos jį patvirtina.

24. Saugos įgaliotinis, siekdamas užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per dvejus metus organizuoja Registro informacinių technologijų saugos atitikties vertinimą.

25. Registro informacinių technologijų saugos atitikties vertinimo metodiką nustato krašto apsaugos ministras.

26. Ne vėliau kaip per 3 darbo dienas nuo Registro informacinių technologijų saugos atitikties vertinimo atlikimo dienos Saugos įgaliotinis parengia Registro atitikties vertinimo ataskaitą bei pastebėtų trūkumų šalinimo planą ir juos ne vėliau kaip per 2 darbo dienas nuo jų parengimo dienos pateikia Registro tvarkytojo vadovui. Registro tvarkytojo vadovas ne vėliau kaip per 3 darbo dienas nuo Registro atitikties vertinimo ataskaitos bei pastebėtų trūkumų šalinimo plano gavimo dienos juos patvirtina.

27. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, Registro saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

28. Registro tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su Registro duomenų tvarkymu, Registro naudotojų ir pačios įrangos administravimu.

29. Registro tarnybinėse stotyse ir kompiuterizuotose vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą, kurios turi būti atsinaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas.

30. Registro programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

31. Naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi Administratoriaus posistemėje Registro tvarkytojo Instituto nustatyta tvarka.

32. Tiesioginė prieiga prie Registro duomenų suteikiama automatiniu būdu ištisą parą darbo ir poilsio dienomis, įgyvendinus Naudotojų autentifikavimo priemones.

33. Registro duomenys perduodami automatiniu būdu naudojant saugų duomenų perdavimo protokolą realiuoju laiku arba asinchroniniu režimu pagal Registro duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, kopijų skaičius, kitos duomenų perdavimo sąlygos ir tvarka.

34. Naudotojai, savo tarnybinėms funkcijoms vykdyti naudojantys nešiojamuosius kompiuterius, Registro duomenis perduodami kompiuterių tinklais ne savo darbo vietoje turi naudoti kompiuterio įjungimo slaptažodį, papildomą Naudotojo tapatybės patvirtinimą ir registro duomenų šifravimą.

35. Kompiuterių tinklo tarnybinės stotys bei kiekvienas kompiuterių tinklui priklausantis kompiuteris privalo turėti užkardą, ribojančią priėjimą iš išorės bei duomenų srautus į išorę. Turi būti draudžiama naudoti interneto ryšį visoms programoms, kurios gali visiškai atlikti savo funkcijas ir be internetinio ryšio su išore. Visi nenaudojami prievadai turi būti užblokuoti.

36. Administratorius atsako už atsarginių Registro duomenų kopijų darymą ir saugojimą automatiniu būdu. Atkurti šią informaciją turi teisę tik Administratorius. Turi būti periodiškai atliekama kopijų tinkamumo ir saugojimo kontrolė.

37. Turi būti užtikrintas saugos incidentų, įvykusių Registre, registravimas, valdymas ir tyrimas Kibernetinio saugumo reikalavimų aprašo ir Visuomenės sveikatos priežiūros specialistų registro veiklos tęstinumo valdymo plano, patvirtinto Lietuvos Respublikos sveikatos apsaugos ministro 2016 m. liepos 12 d. įsakymu Nr. V-926 „Dėl Visuomenės sveikatos priežiūros specialistų registro naudotojų administravimo taisyklių, Visuomenės sveikatos priežiūros specialistų registro saugaus elektroninės informacijos tvarkymo taisyklių ir Visuomenės sveikatos priežiūros specialistų registro veiklos tęstinumo valdymo plano patvirtinimo“, nustatyta tvarka.

38. Registruojami Registre įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis pagal kompetenciją saugos incidentai valdomi, tiriami ir šalinami bei atkuriama Registro veikla.

39. Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą Kibernetinio saugumo reikalavimų aprašo nustatyta tvarka.

40. Perkant paslaugas, įrangą ar darbus, susijusius su Registru, jo projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas privalo laikytis Saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį Kibernetinio saugumo reikalavimų aprašo reikalavimams.

41. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarties vykdymui, nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija yra konfidenciali, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

42. Saugos įgaliotiniu, Kibernetinio saugumo vadovu 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, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

43. Saugos įgaliotinis, Kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, darbą su kompiuterių tinklais, turėti darbo su operacinėmis sistemomis, taikomosiomis programomis patirties, tobulinti kvalifikaciją elektroninės informacijos saugos ir kibernetinio saugumo srityje. Savo darbe turi vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Kibernetinio saugumo reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

44. Administratorius privalo išmanyti pagrindinius saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugumą, turėti sisteminių programinių priemonių administravimo bei priežiūros patirties.

45. Administratorius turi būti susipažinęs su Saugos nuostatais, Saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

46. Naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro duomenis Registro nuostatų nustatyta tvarka ir būti susipažinę su šiais Saugos nuostatais ir Saugos politiką reglamentuojančiais dokumentais.

47. Naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti Saugos įgaliotiniui, Kibernetinio saugumo vadovui ir (arba) Administratoriui.

48. Saugos įgaliotinis ne rečiau kaip kartą per metus inicijuoja Naudotojų mokymą elektroninės informacijos ir kibernetinio saugumo klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos ir kibernetinio saugumo problemas.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

49. Tvarkyti Registro duomenis gali tik įgalioti Naudotojai, kurie yra susipažinę su Saugos dokumentais ir pasirašytinai sutikę laikytis juose nustatytų reikalavimų.

50. Paskyrus Administratorių ir/ar suteikus Naudotojams prieigos teisę naudotis Registro duomenimis, Saugos įgaliotinis nedelsiant supažindina juos su Saugos dokumentais ar kitais Saugos politiką įgyvendinančiais teisės aktais.

51. Saugos įgaliotinis informuoja Administratorių ir Naudotojus apie Saugos dokumentų ar kitų Saugos politikos įgyvendinamųjų teisės aktų pakeitimus ne vėliau kaip per 2 darbo dienas

nuo jų priėmimo dienos. Informacija apie minėtų teisės aktų pakeitimus siunčiama elektroniniu būdu. Pakartotinai su šiais Saugos nuostatais, Saugos dokumentais Administratorius ir Naudotojai pasirašytinai supažindinami tik iš esmės jiems pasikeitus.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

52. Saugos įgaliotinis, Kibernetinio saugumo vadovas, Administratorius ir Naudotojai, pažeidę Saugos dokumentų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

_____