Suvestinė redakcija nuo 2023-05-09

Įsakymas paskelbtas: TAR 2016-03-23, i. k. 2016-05780

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL VISUOMENĖS SVEIKATOS PRIEŽIŪROS SPECIALISTŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2016 m. kovo 22 d. Nr. V-372
Vilnius

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, 9 punktu ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

Preambulės pakeitimai:
Nr. V-1005, 2018-09-11, paskelbta TAR 2018-09-12, i. k. 2018-14405
Nr. V-534, 2023-05-08, paskelbta TAR 2023-05-08, i. k. 2023-08697

1. T v i r t i n u Visuomenės sveikatos priežiūros specialistų registro duomenų saugos nuostatus (pridedama).

2. P a v e d u:

2.1. Higienos institutui per 2 mėnesius nuo šio įsakymo įsigaliojimo dienos:

2.1.1. paskirti visuomenės sveikatos priežiūros specialistų registro duomenų valdymo įgaliotinį, saugos įgaliotinį ir administratorių;

2.1.2. pateikti Lietuvos Respublikos sveikatos apsaugos ministrui tvirtinti:

2.1.2.1. Visuomenės sveikatos priežiūros specialistų registro naudotojų administravimo taisyklių projektą;

2.1.2.2. Visuomenės sveikatos priežiūros specialistų registro saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.1.2.3. Visuomenės sveikatos priežiūros specialistų registro veiklos tęstinumo valdymo plano projektą;

2.2. šio įsakymo vykdymo kontrolę viceministrui pagal veiklos sritį.

Sveikatos apsaugos ministras Juras Požela

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugpjūčio 28 d. raštu Nr. (4.2) 6K-519
Pastraipos pakeitimai:
Nr. V-1005, 2018-09-11, paskelbta TAR 2018-09-12, i. k. 2018-14405

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2016 m. kovo 22 d. įsakymu Nr. V-372
(Lietuvos Respublikos sveikatos apsaugos
ministro 2023 m. gegužės 8 d.
įsakymo Nr. V-534 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).

2. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), vartojamas sąvokas.

3. Registro elektroninės informacijos saugumo ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) tikslas – užtikrinti Registro elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą ir sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro elektroninę informaciją.

4. Elektroninės informacijos saugos politika įgyvendinama 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“ (toliau visi kartu – saugos dokumentai).

5. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. Registro elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo lygio užtikrinimas;

5.2. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Registro elektroninei informacijai tvarkyti, ir saugaus darbo su duomenimis priemonių įgyvendinimas ir kontrolė;

5.3. Registre tvarkomų asmens duomenų apsauga;

5.4. prieigos prie Registro elektroninės informacijos kontrolė;

5.5. Registro veikos tęstinumo užtikrinimas.

6. Saugos nuostatų reikalavimai taikomi:

6.1. Registro valdytojui – Lietuvos Respublikos sveikatos apsaugos ministerijai, Vilniaus g. 33, LT-01506 Vilnius;

6.2. Registro tvarkytojams:

6.2.1. pagrindiniam Registro tvarkytojui – Higienos institutui, Studentų g. 45A, LT- 08107 Vilnius;

6.2.2. kitiems Registro tvarkytojams – Lietuvos nacionalinės sveikatos sistemos visuomenės sveikatos priežiūros įstaigoms (toliau – įstaigos), pavaldžioms Registro valdytojui;

6.3. Registro duomenų valdymo įgaliotiniui;

6.4. Registro administratoriui (toliau – administratorius);

6.5. Registro saugos įgaliotiniui (toliau – saugos įgaliotinis);

6.6. Registro naudotojams (toliau – naudotojai);

6.7. paslaugų, susijusių su Registro veikimu, teikėjams;

6.8. asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Higienos institute tvarkomuose registruose ir informacinėse sistemose (toliau – kibernetinio saugumo vadovas).

7. Už elektroninės informacijos saugą pagal kompetenciją atsako Registro valdytojas ir tvarkytojai.

8. Registro valdytojo funkcijos:

8.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

8.2. priima sprendimus dėl techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.3. tvirtina su Lietuvos Respublikos krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, suderintus Registro saugos dokumentus ir kitus teisės aktus, kuriuose reglamentuojamas Registro elektroninės informacijos tvarkymo teisėtumas ir sauga;

8.4. analizuoja Registro tvarkytojų pasiūlymus dėl Registro elektroninės informacijos saugos priemonių tobulinimo ir priima sprendimus dėl jų finansavimo;

8.5. organizuoja Registro veiklą ir jai vadovauja;

8.6. paveda pagrindiniam Registro tvarkytojui paskirti Registro duomenų valdymo įgaliotinį, Registro administratorių, Registro saugos įgaliotinį ir kibernetinio saugumo vadovą;

8.7. priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.8. kontroliuoja, kaip laikomasi Registro saugos dokumentuose ir kituose elektroninės informacijos saugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų;

8.9. atlieka kitas teisės aktuose, reglamentuojančiuose valstybės registrų ir informacinių sistemų saugą, valdytojui priskirtas funkcijas.

9. Pagrindinio Registro tvarkytojo funkcijos:

9.1. Registro valdytojo pavedimu skiria Registro saugos įgaliotinį, Registro administratorių, kibernetinio saugumo vadovą ir Registro duomenų valdymo įgaliotinį;

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

9.3. užtikrina, kad Registro naudotojai, turintys teisę naudotis Registro elektronine informacija, laikytųsi reikalavimų, nustatytų Registro saugos dokumentuose;

9.4. teikia pasiūlymus Registro valdytojui dėl Registro techninių, programinių priemonių, skirtų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo; organizuoja jų įdiegimą ir modernizavimą;

9.5. pagal kompetenciją atsako už Registro duomenų tvarkymo teisėtumą ir saugų Registro duomenų perdavimą kompiuterių tinklais;

9.6. teikia pasiūlymus Registro valdytojui dėl Registro elektroninės informacijos saugos tobulinimo, Registro saugos dokumentų, kitų teisės aktų, kuriuose reglamentuojamas Registro elektroninės informacijos tvarkymo teisėtumas ir sauga, priėmimo, keitimo arba panaikinimo, taip pat rengia šių dokumentų projektus;

9.7. atlieka Registro duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Registro veikimą;

9.8. užtikrina saugią Registro sąveiką su kitomis informacinėmis sistemomis ir registrais;

9.9. atlieka kitas Registro valdytojo pavestas ir Registro nuostatų, Registro saugos dokumentų bei kitų elektroninės informacijos saugos politiką įgyvendinančių teisės aktų jam priskirtas funkcijas.

10. Kitų Registro tvarkytojų funkcijos ir atsakomybė:

10.1. paskiria asmenį, atsakingą už Registro duomenų tvarkymą, organizacinių ir techninių saugos reikalavimų laikymąsi ir bendradarbiavimą su pagrindiniu Registro tvarkytoju (toliau – Registro tvarkytojo įgaliotas asmuo);

10.2. užtikrina Registro naudotojų laikymąsi Registro saugos dokumentuose nurodytų reikalavimų bei darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių elektroninės informacijos saugą, diegimo koordinavimą ir priežiūrą;

10.3. atlieka kitas Registro valdytojo pavestas ir Registro nuostatų bei Registro saugos dokumentų priskirtas funkcijas.

11. Registro duomenų valdymo įgaliotinio funkcijos:

11.1. atlieka funkcijas, nustatytas Valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 2 dalyje, ir kitas Registro saugos dokumentuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir jam priskirtas funkcijas;

11.2. prireikus pagal kompetenciją teikia pasiūlymus Registro saugos įgaliotiniui dėl saugos nuostatų 44 ir 45 punktuose nurodytų mokymų organizavimo Registro naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais.

12. Registro administratoriaus funkcijos ir atsakomybė:

12.1. suteikia teisę Registro naudotojams naudotis elektronine informacija, reikalinga jų priskirtoms funkcijoms atlikti;

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

12.3. informuoja Registro saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

12.4. diegia ir prižiūri programinę įrangą, reikalingą pagrindinio Registro tvarkytojo funkcijoms vykdyti;

12.5. atsako, kad tvarkant Registrą, nebūtų pažeisti Registro saugos nuostatų reikalavimai;

12.6. organizuoja Registro kompiuterinės ir programinės įrangos administravimą ir priežiūrą, užtikrina kokybišką, tinkamą jos veikimą ir pagal kompetenciją nustato pažeidžiamas Registro vietas;

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

12.8. atlieka kitas pagrindinio Registro tvarkytojo vadovo, Registro saugos įgaliotinio pavestas ir Registro saugos dokumentų jam priskirtas funkcijas.

13. Registro saugos įgaliotinio funkcijos ir atsakomybės:

13.1. teikia pasiūlymus Registro valdytojui dėl Registro saugos dokumentų priėmimo, keitimo ar panaikinimo;

13.2. teikia Registro administratoriui ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

13.3. supažindina Registro administratorių ir Registro naudotojus su Registro saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

13.4. organizuoja Registro informacinių technologijų saugos atitikties vertinimą ir parengia saugos atitikties vertinimo ataskaitą;

13.5. organizuoja kasmetinį Registro rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą;

13.6. koordinuoja ir prižiūri Registro elektroninės informacinės saugos politikos įgyvendinimą;

13.7. organizuoja Registro informacinių technologijų saugos atitikties vertinimą ir parengia saugos atitikties vertinimo ataskaitą;

13.8. atlieka kitas pagrindinio Registro tvarkytojo vadovo pavestas funkcijas.

14. Registro naudotojo funkcijos:

14.1. Registro saugos dokumentų nustatyta tvarka pagal kompetenciją naudojasi ir tvarko elektroninę informaciją, reikalingą jo funkcijoms atlikti;

14.2. informuoja Registro saugos įgaliotinį apie elektroninės informacijos saugos incidentus, o Registro administratorių – apie Registro darbo sutrikimus;

14.3. atlieka kitas Registro saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas funkcijas.

15. Kibernetinio saugumo vadovas vykdo šias funkcijas:

15.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

15.2. atlieka kitas Registro saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

16. Registro elektroninė informacija tvarkoma ir užtikrinamas jos saugumas vadovaujantis:

16.1. Valstybės informacinių išteklių valdymo įstatymu;

16.2. Kibernetinio saugumo įstatymu;

16.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

16.4. Kibernetinio saugumo reikalavimų aprašu;

16.5. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu ir Informacinių technologijų saugos atitikties vertinimo metodika, patvirtintais Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Saugos atitikties vertinimo metodika);

16.6. Saugos dokumentų turinio gairių 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“;

16.7. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių 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 – Klasifikavimo gairių aprašas);

16.8. Visuomenės sveikatos priežiūros specialistų registro nuostatais;

16.9. kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugos politiką ir Registro duomenų tvarkymo teisėtumą bei saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Klasifikavimo gairių aprašo reikalavimais:

17.1. Registre tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai;

17.2. pagal Registre tvarkomos elektroninės informacijos svarbą Registras priskiriamas trečios kategorijos informacinėms sistemoms.

18. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius Registro duomenų vientisumui, konfidencialumui ir prieinamumui. Registro 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. Registro saugos įgaliotinis gali organizuoti neeilinį Registro rizikos įvertinimą.

19. Registro rizikos vertinimas pateikiamas rizikos vertinimo ataskaitoje, kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos Registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Kartu su Registro rizikos vertinimu gali būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Registro kibernetiniam saugumui, vertinimas. Svarbiausieji rizikos veiksniai nurodyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše.

20. Registro rizikos veiksniams vertinti naudojama penkiabalė rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

20.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

20.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

20.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

20.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

20.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

21. Registro rizikos įvertinimo rezultatus saugos įgaliotinis pateikia rizikos įvertinimo ataskaitoje, kurią tvirtina pagrindinio Registro tvarkytojo vadovas. Prireikus tvirtinamas rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Patvirtintos rizikos įvertinimo ataskaitos ir rizikos valdymo priemonių plano, jei toks buvo parengtas, kopijas pagrindinis Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS).

23. Elektroninės informacijos saugos priemonių parinkimo principai:

23.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

23.2. saugos priemonės diegimo kaina turi būti adekvati saugomos elektroninės informacijos vertei;

23.3. kur galima, turi būti įdiegiamos prevencinės elektroninės informacijos saugos priemonės;

23.4. parenkamos tokios saugos priemonės, kad būtų užtikrintas Registro veiklos tęstinumas ir saugus Registro darbas, patiriant kuo mažiau išlaidų.

24. Siekiant įvertinti saugos dokumentuose išdėstytų reikalavimų įgyvendinimo kontrolę, vadovaujantis Saugos atitikties vertinimo metodika kartą per metus organizuojamas Registro informacinių technologijų saugos atitikties vertinimas naudojantis ARSIS.

25. Atlikus Registro informacinių technologijų saugos atitikties vertinimą, rengiama Registro informacinių technologijų saugos atitikties vertinimo ataskaita, prireikus – pastebėtų trūkumų šalinimo planas, kuriuos tvirtina pagrindinis Registro tvarkytojas.

26. Informacinių technologijų saugos atitikties vertinimo ataskaitos kopiją, pastebėtų trūkumų šalinimo plano kopiją pagrindinis Registro tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo turi pateikti ARSIS.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. Programinės įrangos, skirtos Registrą apsaugoti nuo kenksmingosios programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir atnaujinimo reikalavimai:

27.1. Registro tarnybinėse stotyse ir Registro tvarkytojų kompiuterizuotose darbo vietose turi būti naudojamos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą ir atsinaujinančios automatiniu būdu.

27.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

27.3. elektroninės informacijos apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti kenkimo programų apsaugas.

28. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

28.1. naudojama tik legali, Registro funkcijoms vykdyti būtina programinė įranga;

28.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

28.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik Registro administratorius arba Registro tvarkytojo įgaliotas asmuo;

28.4. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Registro elektroninės informacijos, atliktus veiksmus.

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

30. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

30.1. Registro elektroninės informacijos perdavimo tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DoS (angl. *Denial of Service*) ir DDoS (angl. *Distributed Denial of Service*) atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

30.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos;

30.3. pagrindinė Registro duomenų pateikimo prieiga yra duomenų perdavimas šifruotu virtualaus privataus tinklo (VPN) duomenų perdavimo kanalu arba panaudojant saugų HTTPS (angl. *Hypertext Transfer Protocol Secure*) duomenų perdavimo protokolą.

31. Leistinos kompiuterių naudojimo ribos:

31.1. stacionarieji ir nešiojamieji Registro naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš perduodamų remontuoti ar techninei priežiūrai atlikti kompiuterių turi būti pašalinti visi Registro duomenys ir Registro informacija;

31.2. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis, jie turi būti atskirti nuo viešojo interneto tinklo užkarda;

31.3. Registro naudotojai privalo naudotis visomis saugumo priemonėmis apsaugodami kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo, nenaudojami nešiojamieji kompiuteriai turi būti laikomi saugioje vietoje.

32. Metodai, kuriais užtikrinamas saugus Registro elektroninės informacijos teikimas ir (ar) gavimas:

32.1. perduodama Registro elektroninė informacija yra šifruojama naudojant saugų SSL (angl. *Secure Sockets Layer*) protokolą;

32.2. Registro elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP (angl. *Transmission Control Protocol / Internet Protocol*), HTTPS (angl. *Hypertext Transfer Protocol Secure*) protokolus realiuoju laiku; iš susijusių registrų elektroninė informacija gaunama tik pagal duomenų teikimo sutartyse nustatytas sąlygas ir tvarką;

32.3. prieiga prie Registro elektroninės informacijos leidžiama tik per registracijos slaptažodžių sistemą. Prieigos prie Registro elektroninės informacijos valdymas apibrėžtas Registro naudotojų administravimo taisyklėse;

32.4. prieigos prie Registro elektroninės informacijos teises gali suteikti tik Registro administratorius. Registro naudotojams suteikiamos tik jų funkcijoms atlikti būtinos teisės.

33. Pagrindinio Registro tvarkytojo naudotojų kompiuterizuotos darbo vietos turi būti valdomos naudojant centralizuoto valdymo priemones (pvz., katalogų tarnybą „*Active direktory*“).

34. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

34.1. atsarginės elektroninės informacijos kopijos (toliau – kopijos) turi būti daromos automatiniu būdu ne rečiau kaip kas 24 valandas;

34.2. kopijos turi būti saugomos kitoje patalpoje nei yra Registro tarnybinės stotys;

34.3. elektroninė informacija kopijose turi būti šifruojama;

34.4. kopijas turi teisę tvarkyti Registro administratorius arba techninės bei programinės įrangos priežiūros paslaugų teikėjai.

35. Turi būti užtikrintas saugos incidentų, įvykusių Registre, registravimas, valdymas ir tyrimas Kibernetinių saugumo reikalavimų aprašo ir Registro veiklos tęstinumo valdymo plano nustatyta tvarka:

35.1. 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;

35.2. Kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

36. Perkant paslaugas, darbus ar įrangą, 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 turi būti nustatyta, kad asmuo, atliekantis Registro techninės ir programinės įrangos priežiūros ir duomenų, informacijos ir dokumentų ir (arba) jų kopijų tvarkymo funkcijas, negali turėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat negali turėti paskirtos administracinės nuobaudos už Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo yra praėję mažiau kaip vieni metai, taip pat privalo laikytis Registro saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems Kibernetinio saugumo reikalavimų aprašo reikalavimams.

37. 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 sutarčiai vykdyti.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

38. Registro saugos įgaliotinis, kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos ir kibernetinio saugumo srityje, savo darbe turi vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

39. Registro saugos įgaliotiniu, kibernetinio saugumo vadovu negali būti skiriami asmenys, turintys neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai. Registro saugos įgaliotinis ir kibernetinio saugumo vadovas, pažeidęs saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

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

41. Registro administratorius turi būti susipažinęs su saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

42. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Registro duomenis Registro nuostatų nustatyta tvarka ir būti susipažinę su saugos dokumentais.

43. Registro naudotojai, pastebėję saugos reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones Registre, privalo nedelsdami apie tai pranešti Registro administratoriui ar Registro saugos įgaliotiniui.

44. Registro saugos įgaliotinis arba kibernetinio saugumo vadovas ne rečiau kaip kartą per dvejus metus inicijuoja Registro naudotojų mokymą elektroninės informacijos saugos ir kibernetinio saugumo klausimais, prireikus įvairiais būdais – pranešimais elektroniniu paštu, naujų darbuotojų instruktavimu, atmintinių rengimu, teminių seminarų organizavimu ir kitais informavimo būdais – primena apie saugumo problemas.

45. Registro naudotojų mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), Registro naudotojų, Registro duomenų valdymo įgaliotinio ir Registro administratoriaus poreikius.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

46. Tvarkyti Registro duomenis gali tik naudotojai, susipažinę su Registro saugos dokumentais ir raštu pasirašę pasižadėjimus saugoti asmens duomenų paslaptį.

47. Registro saugos įgaliotinis bei kitų Registro tvarkytojų vadovų paskirti atsakingi asmenys atsako už Registro naudotojų supažindinimą su Registro saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

48. Registro saugos įgaliotinis, Registro kibernetinio saugumo vadovas, Registro administratorius ir Registro naudotojai, pažeidę Registro saugos dokumentų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Priedo pakeitimai:
Nr. V-1005, 2018-09-11, paskelbta TAR 2018-09-12, i. k. 2018-14405
Nr. V-534, 2023-05-08, paskelbta TAR 2023-05-08, i. k. 2023-08697

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-1005, 2018-09-11, paskelbta TAR 2018-09-12, i. k. 2018-14405
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

2.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-534, 2023-05-08, paskelbta TAR 2023-05-08, i. k. 2023-08697

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