LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINIŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020m. sausio 2 d. V-3

Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 2 dalimi:

1. T v i r t i n u Sveikatos priežiūros įstaigos informacinės sistemos pavyzdinius duomenų saugos nuostatus (pridedama).

2. R e k o m e n d u o j u Sveikatos priežiūros įstaigos informacinės sistemos pavyzdiniais duomenų saugos nuostatais vadovautis:

2.1. sveikatos priežiūros įstaigoms (viešosioms įstaigoms ir biudžetinėms įstaigoms) rengiant įstaigos valstybės informacinės sistemos duomenų saugos nuostatus;

2.2. privačioms sveikatos priežiūros įstaigoms, kurių informacinės sistemos gauna duomenis iš valstybės informacinių sistemų ar registrų, rengiant privačios sveikatos priežiūros įstaigos informacinės sistemos duomenų saugos nuostatus.

3. P a v e d u įsakymo vykdymą kontroliuoti viceministrui pagal veiklos sritį.

Sveikatos apsaugos ministras Aurelijus Veryga

Sveikatos apsaugos viceministrė
Kristina Garuolienė
2019-12-31

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Vita Korsakienė
2019-12-30

SUDERINTA
Nacionalinio kibernetinio saugumo centro
2019-11-21 raštu Nr. (4.2) 6K-760

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
0-19198 2019-12-19

Teisės skyriaus vyriausiasis specialistas
Marimantas Satkus
2019-12-19
Laikinai vykdanti skyriaus vedėjo funkcijas

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus patarėja
Vilma Telyčėnienė
2019-12-19

Skelbti Teisės aktų registre

Teisės skyriaus vedėja
Martyna Mickė
2019-12-19

E. sveikatos informacinių technologijų koordinavimo ir įgyvendinimo patarėjas
Linas Kavolius
2019 12 19

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2020m. sausio 2 įsakymu Nr. V-3

SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINIAI DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Sveikatos priežiūros įstaigos informacinės sistemos pavyzdiniai duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja _____ (sveikatos priežiūros įstaigos pavadinimas) informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Informacinės sistemos elektroninės informacijos saugos politikos tikslas – užtikrinti Informacinės sistemos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo 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), ir Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. Informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos tvarkymo kontrolė;

5.4. Informacinės sistemos paslaugų ir naudojimosi Informacinės sistemos elektronine informacija kontrolės užtikrinimas;

5.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;

5.6. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.7. Informacinės sistemos naudotojų mokymas.

6. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojai.

7. Informacinės sistemos valdytojas atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

8. Informacinės sistemos tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos politiką įgyvendinančiuose dokumentuose (toliau – saugos dokumentai) nustatyta tvarka.

9. Saugos nuostatai taikomi Informacinės sistemos valdytojui _____ (įstaigos pavadinimas, adresas), Informacinės sistemos pagrindiniam tvarkytojui _____ (įstaigos pavadinimas, adresas), kitiems Informacinės sistemos tvarkytojams: _____ (išvardijami kiti tvarkytojai, jeigu jie yra), Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriams, Informacinės sistemos naudotojams, Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

10. Informacinės sistemos valdytojo _____ (įstaigos pavadinimas) funkcijos:

10.1. organizuoti ir vadovauti informacinių sistemų veiklai;

10.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;

10.3. kontroliuoti, kad Informacinė sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;

10.4. tvirtinti Saugos nuostatus, saugos dokumentus ir kitus teisės aktus, susijusius su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu);

10.5. nagrinėti Informacinės sistemos tvarkytojų pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

10.6. skirti Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorius arba pavesti juos paskirti savo organizacijoje Informacinės sistemos tvarkytojui;

10.7. atlikti kitas Informacinės sistemos nuostatuose ir Saugos nuostatuose nustatytas funkcijas.

11. Pagrindinio Informacinės sistemos tvarkytojo _____ (įstaigos pavadinimas) funkcijos:

11.1. atlikti Informacinės sistemos nuostatuose nustatytas funkcijas;

11.2. užtikrinti nepertraukiamą Informacinės sistemos veiklą;

11.3. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

11.4. pagal kompetenciją prižiūrėti Informacinės sistemos duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus Informacinės sistemos komponentus, užtikrinti jų veikimą;

11.5. užtikrinti saugos dokumentų ir kitų Informacinės sistemos valdytojo priimtų teisės aktų, susijusių su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

11.6. pagal kompetenciją įgyvendinti Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

11.7. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);

11.8. teikti Informacinės sistemos valdytojui pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

11.9. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą ir aktualizavimą;

11.10. atlikti kitas Informacinės sistemos valdytojo pavestas Informacinės sistemos nuostatuose, Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

12. Informacinių sistemų tvarkytojų _____ (išvardinami kiti tvarkytojai, jeigu jie yra) funkcijos:

12.1. pagal kompetenciją prižiūrėti kompiuterius, operacines sistemas ir kitus Informacinės sistemos komponentus savo sveikatos priežiūros įstaigose, užtikrinti jų veikimą;

12.2. užtikrinti administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą Informacinės sistemos naudotojų kompiuteriuose ir kituose Informacinės sistemos komponentuose savo sveikatinimo įstaigose;

12.3. užtikrinti organizacinėmis, techninėmis, technologinėmis ir metodinėmis priemonėmis saugų Informacinės sistemos elektroninės informacijos tvarkymą savo sveikatinimo įstaigose;

12.4. valdyti elektroninės informacijos saugos (kibernetinius) incidentus savo sveikatinimo įstaigose ir juos šalinti;

12.5. užtikrinti saugos dokumentų ir kitų Informacinės sistemos valdytojo priimtų teisės aktų, susijusių su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

12.6. pagal kompetenciją įgyvendinti Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus savo sveikatinimo įstaigose;

12.7. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą) savo sveikatinimo įstaigose;

12.8. pagal kompetenciją atlikti kitas Informacinės sistemos valdytojo pavestas Informacinės sistemos nuostatuose, Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

13. Informacinės sistemos saugos įgaliotinio funkcijos:

13.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

13.2. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

13.3. atlikti 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 – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.4. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;

13.5. organizuoti Informacinės sistemos rizikos įvertinimą ir parengti rizikos įvertinimo ataskaitą;

13.6. supažindinti Informacinės sistemos administratorius ir Informacinės sistemos naudotojus su Saugos nuostatų ir saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

13.7. organizuoti Informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoti juos apie elektroninės informacijos saugos problemas;

13.8. duoti Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Saugos nuostatų ir saugos dokumentų įgyvendinimu;

13.9. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui pasiūlymus dėl koordinuojančio Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

13.10. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą savo sveikatos priežiūros įstaigose ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

13.11. teikti Informacinės sistemos administratoriams ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

13.12. atlikti kitas Informacinės sistemos pagrindinio tvarkytojo vadovo pavestas Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

14. Saugos įgaliotinis negali atlikti Informacinės sistemos administratoriaus funkcijų.

15. Informacinės sistemos administratoriaus funkcijos:

15.1. užtikrinti Informacinės sistemos techninės ir programinės įrangos įdiegimą ir funkcionavimą;

15.2. diegti ir prižiūrėti programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

15.3. suteikti teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

15.4. užtikrinti Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustatyti Informacinės sistemos pažeidžiamas vietas;

15.5. pagal kompetenciją dalyvauti vykdant saugumo reikalavimų įgyvendinimo stebėseną;

15.6. pagal kompetenciją teikti Informacinės sistemos tvarkytojo vadovui siūlymus dėl Informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

15.7. informuoti Informacinės sistemos saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikti siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

15.8. daryti Informacinės sistemos duomenų bazės atsargines kopijas ir atsakyti už archyve esančių kopijų saugojimą;

15.9. atlikti kitas Informacinės sistemos pagrindinio tvarkytojo vadovo ir saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

16. Teisės aktai, kuriais vadovaujamasi tvarkant informacinių sistemų elektroninę informaciją ir užtikrinant jos saugą:

16.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1);

16.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

16.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

16.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

16.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

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

16.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

16.8. Techniniai elektroninės informacijos saugos reikalavimai;

16.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių

technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

16.10. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

16.11. Saugos nuostatai, saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 7–10 punktais, Informacinės sistemos tvarkoma informacija priskiriama prie _____ (įrašoma nustatyta informacijos svarbos kategorija).

18. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12 punktu, Informacinė sistema priskiriama prie _____ (įrašoma nustatyta Informacinės sistemos svarbos kategorija).

19. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

20. Organizuojant rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas Informacinės sistemos pagrindinio tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

21. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai:

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

21.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo 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. Informacinės sistemos rizikos veiksniams vertinti naudojama dvidešimt penkių balų rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

22.1. rizikos laipsnis nuo 1 iki 6 – maža rizika;

22.2. rizikos laipsnis nuo 8 iki 12 – vidutinė rizika;

22.3. rizikos laipsnis nuo 15 iki 25 – didelė rizika.

23. Kuo didesnė rizikos veiksnio tikimybė ir jo poveikis, tuo rizikos laipsnis aukštesnis. Rizikos veiksniams, kuriems nustatytas aukštas rizikos laipsnis, būtina skirti didžiausią dėmesį parenkant ir įgyvendinant tinkamas rizikos mažinimo priemones.

24. Informacinės sistemos rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama Informacinės sistemos pagrindinio tvarkytojo vadovui. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

25. Atsižvelgdamas į rizikos vertinimo ataskaitą, Informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

27. Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Informacinės sistemos pagrindinio tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus jo vykdytojus paskiria ir įgyvendinimo terminus nustato Informacinės sistemos valdytojo vadovas.

28. Informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

29. Informacinės sistemos rizikos įvertinimo ataskaitos, Informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, taip pat pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo 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 krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka (jeigu Informacinė sistema priskiriama valstybės informaciniams ištekliams).

30. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais principais:

30.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

30.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

30.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

31. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 17 ir 18 punktuose nustatytas Informacinės sistemos svarbos kategorijas ir vadovaujantis Saugos nuostatų 16 punkte nurodytais teisės aktais ir standartais.

32. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerosios saugumo praktikos rekomendacija.

33. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Informacinės sistemos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

34. Programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

34.1. Informacinės sistemos tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai ir operatyviai atnaujinamos automatiniu būdu;

34.2. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų;

34.3. _____ (nurodomos kitos galimos programinės įrangos naudojimo nuostatos ir jos atnaujinimo reikalavimai).

35. Detalios programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas ir kt.), nustatomi Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

36. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

36.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

36.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

36.3. turi būti įdiegta prieigos prie Informacinės sistemos elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

36.4. turi būti įgyvendinta prievolė keisti slaptažodžius ne rečiau kaip _____ (nurodomas slaptažodžių keitimo periodiškumas);

36.5. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Informacinės sistemos elektroninės informacijos, atliktus veiksmus;

36.6. _____ (nurodomos kitos galimos programinės įrangos naudojimo nuostatos).

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

37.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

37.2. Informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: _____ (nurodomos galimos per tinklą vykdomų atakų rūšys);

37.3. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

37.4. _____ (nurodomos kitos galimos kompiuterių tinklo filtravimo įrangos naudojimo nuostatos).

38. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

39. Leistinos kompiuterių naudojimo ribos:

39.1. stacionarūs ir nešiojamieji Informacinės sistemos naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Informacinės sistemos duomenys ir informacija;

39.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.);

39.3. Informacinės sistemos naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo;

39.4. _____ (nurodomos kitos galimos kompiuterių naudojimo ribos).

40. Metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos teikimas ir (ar) gavimas:

40.1. elektroninė informacija iš susijusių registrų, informacinių sistemų gaunama ir teikiama susijusiems registrams, informacinėms sistemoms tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

40.2. prieigos prie Informacinės sistemos elektroninės informacijos teises gali suteikti tik Informacinės sistemos administratorius. Informacinės sistemos naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

40.3. prieiga prie Informacinės sistemos elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie Informacinės sistemos elektroninės informacijos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse;

40.4. pasibaigus Informacinės sistemos naudotojo darbo sutarčiai, teisė naudotis Informacinės sistemos elektronine informacija turi būti panaikinta. Informacinės sistemos naudotojui prieiga prie Informacinės sistemos turi būti ribojama ar sustabdoma, kai vyksta Informacinės sistemos naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos;

40.5. _____ (nurodomi kiti galimi metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos teikimas ir (ar) gavimas).

41. Informacinės sistemos atsarginės duomenų bazės kopijos daromos automatiniu būdu _____ (nurodomas periodiškumas), esant aktyviai Informacinės sistemos duomenų bazei. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos.

42. Prireikus atkurti kopijas teisę tam turi tik Informacinės sistemos administratorius ar jį pavaduojantis asmuo. Periodiškai, bet ne rečiau kaip kartą per pusmetį turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai. Patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

43. Kopijų darymo ir saugojimo tvarka nustatoma Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

44. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami Informacinės sistemos saugos (kibernetinio saugumo) politiką įgyvendinančiuose dokumentuose.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

45. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą

(kibernetinį saugumą). Informacinės sistemos tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

46. 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 prijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

47. Informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti Informacinės sistemos komponentus (stebėti Informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Informacinės sistemos administratoriai turi būti susipažinę su saugos dokumentais.

48. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

49. Informacinės sistemos naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybės aprašyme.

50. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

50.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams, informacinių sistemų administratoriams ir pan.);

50.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, Informacinės sistemos naudotojų ar informacinių sistemų administratorių poreikius;

50.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

50.4. mokymai Informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis. Mokymai Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

51. Informacinės sistemos naudotojus su Saugos nuostatais ir saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindina Informacinės sistemos saugos įgaliotinis. Informacinės sistemos naudotojai, pažeidę Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

52. Pakartotinai su Saugos nuostatais ir saugos dokumentais Informacinės sistemos naudotojai supažindinami jiems pasikeitus.

53. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Informacinės sistemos tvarkytojo interneto svetainėje ar kitais būdais.

54. Informacinės sistemos naudotojų supažindinimo su Saugos nuostatais ir saugos dokumentais tvarka nustatyta Informacinės sistemos naudotojų administravimo taisyklėse.

55. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik Informacinės sistemos naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų. Informacinės sistemos naudotojai atsako už Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

56. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

57. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru. Keičiami saugos dokumentai gali būti nederinami su Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos šių dokumentų kopijos.

58. Saugos nuostatai ir saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Vita Korsakienė
2019-12-30

Lietuvos Respublikos Sveikatos apsaugos ministras
Aurelijus Veryga
2020-01-02

Teisės skyriaus vyriausiasis specialistas
Narimantas Satkus
2019-12-19

E. sveikatos informacinių technologijų koordinavimo ir įgyvendinimo patarėjas
Linas Kavolius
2019-12-19

Teisės skyriaus vedėja
Martyna Mickė
2019-12-19

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2019-12-19

Einantis skyriaus vedėjo funkcijas
Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus patarėja
2019-12-19
Vilma Telyčėnienė