*Suvestinė redakcija nuo 2021-11-20*

*Įsakymas paskelbtas: TAR 2021-11-12, i. k. 2021-23506*

**NACIONALINIO VISUOMENĖS SVEIKATOS CENTRO PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIUS**

# ĮSAKYMAS DĖL UŽKREČIAMŲJŲ LIGŲ IR JŲ SUKĖLĖJŲ VALSTYBĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2021 m. lapkričio 12 d. Nr. VKE-561
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 5 punktu, 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, 8, 11, 19 ir 26 punktais, 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“, 5.3 papunkčiu, Lietuvos Respublikos sveikatos apsaugos ministro 2021 m. spalio 22 d. įsakymu Nr. V-2390 „Dėl Užkrečiamųjų ligų ir jų sukėlėjų valstybinės informacinės sistemos modernizavimo, Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos nuostatų patvirtinimo“ bei Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. rugsėjo 18 d. įsakymu Nr. V-1058 „Dėl Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos nuostatų patvirtinimo“, 16.3 papunkčiu:

1. T v i r t i n u Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos duomenų saugos nuostatus (pridedama).

2. S k i r i u:

2.1. Informacinių sistemų valdymo skyriaus informacinių technologijų ir ryšių saugumo specialistą Artūrą Žižį Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos (toliau – Informacinė sistema) saugos įgaliotiniu;

2.2. Užkrečiamųjų ligų valdymo skyriaus kompiuterių sistemų administratorių Viktorą Bumšteiną Informacinės sistemos administratoriumi;

2.3. Užkrečiamųjų ligų valdymo skyriaus patarėją Rasą Liausėdienę Informacinės sistemos duomenų valdymo įgaliotine.

3. P a v e d u:

3.1. šio įsakymo 2 punkte įvardintiems darbuotojams pagal paskirtas atsakomybes vykdyti jiems teisės aktais numatytas funkcijas;

3.2. Informacinių sistemų valdymo skyriaus informacinių technologijų ir ryšių saugumo specialistui Artūrui Žižiui ne vėliau kaip per 1 (vieną) mėnesį nuo šio įsakymo įsigaliojimo dienos parengti Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles, Informacinės

sistemos veiklos tęstinumo valdymo planą ir Informacinės sistemos naudotojų administravimo taisykles.

4. Į p a r e i g o j u:

4.1. Kokybės vadybos ir komunikacijos skyriaus patarėją Brigitą Kairienę ne vėliau kaip per 1 (vieną) darbo dienas nuo įsakymo užregistravimo dienos dokumentų valdymo sistemos (toliau – DVS) priemonėmis supažindinti su šiuo įsakymu direktoriaus pavaduotoją, skyrių, neįeinančių į departamentų sudėtį, vedėjus, departamentų direktorius ir darbuotojus, nurodytus šio įsakymo 2 punkte;

4.2. skyrių, neįeinančių į departamentų sudėtį, vedėjus ne vėliau kaip per 3 (tris) darbo dienas nuo įsakymo užregistravimo dienos su šiuo įsakymu DVS priemonėmis supažindinti vadovaujamo skyriaus valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis;

4.3. departamentų direktorius ne vėliau kaip per 3 (tris) darbo dienas nuo įsakymo užregistravimo dienos su šiuo įsakymu DVS priemonėmis supažindinti vadovaujamo departamento valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis.

5. P r i p a ž į s t u netekusiais galios:

5.1. Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos direktoriaus 2020 m. rugpjūčio 21 d. įsakymą Nr. VKE-363 „Dėl Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos saugos įgaliotinio, administratoriaus ir duomenų valdymo įgaliotinio paskyrimo“ su visais jo pakeitimais;

5.2. Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos direktoriaus 2020 m. spalio 7 d. įsakymą Nr. VKE-443 „Dėl Užkrečiamųjų ligų ir jų sukėlėjų valstybinės informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

6. P a s i l i e k u įsakymo vykdymo kontrolę.

Užkrečiamųjų ligų valdymo skyriaus vedėja,
laikinai vykdanti direktoriaus funkcijas — Giedrė Aleksienė

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021-11-08 raštu Nr. (4.1 E)6K-883

PATVIRTINTA
Nacionalinio visuomenės sveikatos centro prie
Sveikatos apsaugos ministerijos
direktoriaus 2021 m. lapkričio 12 d.
įsakymu Nr. VKE-561

# UŽKREČIAMŲJŲ LIGŲ IR JŲ SUKĖLĖJŲ VALSTYBĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Užkrečiamųjų ligų ir jų sukėlėjų valstybės 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 Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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 – 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. Informacinėje sistemoje tvarkomų asmens duomenų apsauga;

5.6. Informacinės sistemos veikos tęstinumo užtikrinimas;

5.7. Informacinės sistemos naudotojų mokymas.

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

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 tvarkytojas 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 (toliau – Valdytojas) ir Informacinės sistemos tvarkytojui (toliau – Tvarkytojas), Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriui, Informacinės sistemos duomenų valdymo įgaliotiniui, Informacinės sistemos naudotojams, Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

10. Valdytojas ir Tvarkytojas yra Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, Kalvarijų g. 153, LT-08221, Vilnius.

11. Valdytojo funkcijos:

11.1. organizuoti ir vadovauti informacinių sistemų veiklai;

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

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

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

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

11.6. skirti Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorių;

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

12. Tvarkytojo funkcijos:

12.1. atlikti Informacinės sistemos nuostatuose nustatytas funkcijas;

12.2. užtikrinti nepertraukiamą Informacinės sistemos veiklą;

12.3. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

12.4. 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;

12.5. užtikrinti saugos dokumentų ir kitų 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;

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

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

12.9. užtikrinti administracinių, techninių ir organizacinių saugos priemonių, skirtų elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, įgyvendinimą;

12.10. valdyti elektroninės informacijos saugos (kibernetinius) incidentus ir juos šalinti;

12.11. atlikti kitas 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 valdytojo 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 valdytojo 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 administratorių 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 valdytojo vadovui pasiūlymus dėl koordinuojančio Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

13.10. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės 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 administratoriui ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

13.12. atlikti kitas Informacinės sistemos valdytojo 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 bei programinės įrangos įdiegimą ir funkcionavimą;

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

15.3. įgyvendinti 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, įsilaužimų 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 valdytojo 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 valdytojo vadovo ir saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

16. Teisės aktai, kuriais vadovaujamasi tvarkant Informacinės sistemos elektroninę informaciją ir užtikrinant jos saugumą:

16.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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);

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 sistemų klasifikavimo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

16.8. Techninių Valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas ir informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta 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“;

16.9. Lietuvos standartai LST ISO/IEC 27001, LST ISO/IEC 27002 ir kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, apibrėžiantys saugų duomenų tvarkymą;

16.10. 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, 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 ir 12 punktais:

17.1. vadovaujantis Klasifikavimo gairių aprašo 9 punktu, Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama vidutinės svarbos informacijos kategorijai. Priskyrimo šiai elektroninės informacijos svarbos kategorijai kriterijai: dėl informacijos konfidencialumo, vientisumo ir (ar) prieinamumo praradimo gali kilti grėsmė, kad prasidės procesai, galintys pažeisti daugiau nei 1 procento, bet ne daugiau nei 5 procentų valstybės gyventojų teises ir teisėtus interesus bei lemti, kad nebus atliekama funkcija ministrui pavestoje valdymo srityje;

17.2. vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčiu, Informacinė sistema priskiriama trečiajai informacinių sistemų kategorijai.

18. 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.

19. 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.

20. 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:

20.1. 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);

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

20.3. 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.

21. Informacinės sistemos rizikos veiksniams vertinti naudojama dvidešimt penkių balų rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

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

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

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

22. 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.

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

24. 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.

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

26. 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.

27. 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.

28. 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.

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

29.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

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

## III SKYRIUS
## ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

31. 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.

32. 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.

33. 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:

33.1. 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;

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

33.3. programinė įranga apsauganti nuo kenksmingos programinės įrangos turi būti nuolat atnaujinama automatiniu būdu ne rečiau kaip kas 16 val.;

33.4. elektroninio pašto tarnybinės stotys turi būti apsaugotos nuo brukalų (angl. *spam*) ir nepageidaujamo turinio elektroninių laiškų.

34. 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.

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

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

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

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

35.4. turi būti įgyvendinta prievolė ne rečiau kaip kas tris mėnesius keisti slaptažodžius;

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

35.6. programinę įrangą, reikalingą Informacinės sistemos naudotojo funkcijoms atlikti, diegia, atnaujina, kontroliuoja ir prižiūri administratorius arba kvalifikuoti paslaugų teikėjų specialistai;

35.7. darbo vietose, kuriose dirbama su Informacine sistema, neturi būti naudojamos programos ir dokumentai, nesusiję su įstaigos funkcijomis ar Informacinės sistemos naudotojo funkcijomis.

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

36.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

36.2. Informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) bei kitų per tinklą vykdomų atakos rūšių;

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

36.4. duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

36.5. turi būti naudojamos turinio filtravimo sistemos.

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

38. Leistinos kompiuterių naudojimo ribos:

38.1. stacionarūs ir nešiojamieji 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;

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

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

38.4. Informacinės sistemos naudotojai turi būti identifikuoti:

38.4.1. slaptažodžiai naudojami visais lygiais – nuo kompiuterio įjungimo iki prisijungimo prie informacinės sistemos;

38.4.2. nustatomi specialūs reikalavimai slaptažodžių sistemai;

38.4.3. slaptažodžiai negali būti atskleidžiami tretiesiems asmenims.

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

39.1. 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;

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

39.3. 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;

39.4. 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;

39.5. prieiga prie Informacinės sistemos turi būti ribojama pagal numatytus kriterijus (IP adresus).

40. Informacinės sistemos atsarginės duomenų bazės kopijos daromos automatiniu būdu kas dieną, 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.

41. Prireikus atkurti kopijas teisę tam turi tik Informacinės sistemos administratorius ar paslaugų teikėjų specialistai. 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.

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

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

## IV SKYRIUS
## REIKALAVIMAI PERSONALUI

44. Informacinės sistemos saugos įgaliotinis privalo:

44.1. išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus;

44.2. tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją;

44.3. 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);

44.4. Informacinės sistemos tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

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

46. Informacinės sistemos administratorius pagal kompetenciją privalo:

46.1. išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą;

46.2. 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;

46.3. sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą;

46.4. Informacinės sistemos administratoriai turi būti susipažinę su saugos dokumentais.

47. Informacinės sistemos naudotojai privalo:

47.1. turėti pagrindinius darbo su kompiuteriu, taikomosiomis programomis įgūdžius;

47.2. mokėti tvarkyti elektroninę informaciją Informacinės sistemos nuostatų nustatyta tvarka;

47.3. būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą;

47.4. 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.

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

49. Informacinės sistemos naudotojų ir Informacinės sistemos administratoriaus mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

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

*Papunkčio numeracijos pakeitimas:*
*Nr. VKE-574, 2021-11-19, paskelbta TAR 2021-11-19, i. k. 2021-23968*

49.2. 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 Informacinės sistemos administratoriaus poreikius;

49.3. 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.);

49.4. Informacinės sistemos naudotojams ir Informacinės sistemos administratoriui mokymus gali vykdyti saugos įgaliotinis ar kitas Informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas;

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

50. Informacinės sistemos naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui ir/arba administratoriui.

51. Informacinės sistemos 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.

## V SKYRIUS
## INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

52. Informacinės sistemos naudotojus su Saugos nuostatais ir saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindina Informacinės sistemos saugos įgaliotinis.

53. Informacinės sistemos naudotojai pakartotinai supažindinami pasikeitus Saugos nuostatams ir / arba saugos dokumentams .

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

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

56. 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.

57. 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

58. 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.

59. 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.

60. Įsigyjant viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas, elektroninės informacijos prieglobos paslaugas, skaitmenines paslaugas, jų teikėjams taikomi reikalavimai, nustatyti 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“.

---

**Pakeitimai:**

1.
Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. VKE-574, 2021-11-19, paskelbta TAR 2021-11-19, i. k. 2021-23968
Dėl korektūros klaidos Nacionalinio visuomenės sveikatos centro prie sveikatos apsaugos ministerijos direktoriaus 2021 m. lapkričio 12 d. įsakyme Nr. VKE-561 „Dėl Užkrečiamųjų ligų ir jų sukėlėjų valstybės informacinės sistemos duomenų saugos nuostatų patvirtinimo“ ištaisymo