Suvestinė redakcija nuo 2023-08-26

Įsakymas paskelbtas: TAR 2020-05-05, i. k. 2020-09530

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS

DĖL UŽKREČIAMŲJŲ LIGŲ, GALINČIŲ IŠPLISTI IR KELTI GRĖSMĘ, STEBĖSENOS IR KONTROLĖS INFORMACINĖS SISTEMOS STEIGIMO IR JOS NUOSTATŲ BEI DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. gegužės 5 d. Nr. V-1067
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsniu, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 11 punktu ir 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, 11, 19 ir 26 punktais:

1. Į s t e i g i u Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinę sistemą.

2. T v i r t i n u pridedamus:

2.1. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos nuostatus;

2.2. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos duomenų saugos nuostatus.

3. N u s t a t a u Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos veikimo pradžią – 2020 m. gegužės 15 d.

4. P a v e d u Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos direktoriui:

4.1. paskirti Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos saugos įgaliotinį, administratorių, duomenų valdymo įgaliotinį;

4.2. per 1 mėnesį nuo šio įsakymo įsigaliojimo parengti ir teisės aktų nustatyta tvarka suderinti bei Lietuvos Respublikos sveikatos apsaugos ministerijai pateikti tvirtinti:

4.2.1. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos naudotojų administravimo taisyklių projektą;

4.2.2. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos elektroninės informacijos tvarkymo taisyklių projektą;

4.2.3. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės

sistemos veiklos tęstinumo valdymo plano projektą.

Sveikatos apsaugos ministras Aurelijus Veryga

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2020 m. gegužės 5 d. įsakymu Nr. V-1067

UŽKREČIAMŲJŲ LIGŲ, GALINČIŲ IŠPLISTI IR KELTI GRĖSMĘ, STEBĖSENOS IR KONTROLĖS INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos nuostatai (toliau – Nuostatai) reglamentuoja Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos (toliau – Informacinė sistema) steigimo teisinį pagrindą, tikslus, uždavinius ir pagrindines funkcijas, organizacinę, informacinę ir funkcinę struktūras, duomenų teikimą ir naudojimą, bendruosius reikalavimus duomenų saugai, finansavimą, modernizavimą ir likvidavimą.

2. Informacinės sistemos steigimo teisinis pagrindas – Lietuvos Respublikos žmonių užkrečiamųjų ligų profilaktikos ir kontrolės įstatymo 6, 8, 9, 19, 20, 21 ir 27 straipsniai.

3. Pagrindiniai teisės aktai, kuriais vadovaujantis kuriama ir tvarkoma Informacinė sistema:

3.1. 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) (toliau – Reglamentas (ES)2016/679);

3.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (toliau – Įstatymas);

3.3. Lietuvos Respublikos sveikatos sistemos įstatymas;

3.4. Lietuvos Respublikos visuomenės sveikatos priežiūros įstatymas;

3.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

3.6. Lietuvos Respublikos kibernetinio saugumo įstatymas;

3.7. Lietuvos Respublikos žmonių užkrečiamųjų ligų profilaktikos ir kontrolės įstatymas;

3.8. Lietuvos Respublikos visuomenės sveikatos stebėsenos (monitoringo) įstatymas;

3.9. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ (toliau – Aprašas);

3.10. Bendrųjų elektroninės informacijos saugos reikalavimų 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“;

3.11. 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“;

3.12. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymu Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“;

3.13. 2020 m. liepos 15 d. Komisijos įgyvendinimo sprendimas (ES) 2020/1023, kuriuo dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi duomenimis kovojant su COVID-19 pandemija iš dalies keičiamas Įgyvendinimo sprendimas (ES) 2019/1765;

Papildyta papunkčiu:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

3.14. Kitais teisės aktais, reglamentuojančiais elektroninės informacijos tvarkymą.

Papunkčio numeracijos pakeitimas:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

4. Nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Nuostatų 3 punkte nurodytuose teisės aktuose.

5. Informacinės sistemos tikslas – informacinių technologijų priemonėmis surinkti, apdoroti ir pateikti analizei epidemiologiškai reikšmingus duomenis, padėsiančius užtikrinti užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėseną ir kontrolę bei tinkamai valdyti ypatingąsias epidemines situacijas.

6. Informacinės sistemos asmens duomenų tvarkymo tikslai:

6.1. epidemiologinė duomenų analizė ir statistika;

6.2. karantino ar izoliavimo reikalavimų laikymasis;

6.3. informavimas apie užkrečiamosios ligos židinį ar apsauginę zoną;

6.4. užkrečiamųjų ligų kontrolė, epidemiologinė priežiūra ir stebėsena (monitoringas);

6.5. *Neteko galios nuo 2020-09-15*

Papunkčio naikinimas:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

6.6. sąlytį turėjusių asmenų išaiškinimas ir jų įspėjimas apie gresiantį pavojų;

6.7. naudotojų administravimas bei identifikavimas;

6.8. *Neteko galios nuo 2020-09-15*

Papunkčio naikinimas:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

7. Informacinės sistemos uždaviniai:

7.1. automatizuoti informacijos apie nustatytus ligos atvejus gavimą ir tinkamai tvarkyti epidemiologiškai reikšmingus duomenis bei asmens duomenis valstybiniu ir teritoriniu lygiu, siekiant užkirsti kelią užkrečiamųjų ligų išplitimui bei tinkamai valdyti ypatingąsias epidemines situacijas;

7.2. automatizuoti informacijos gavimą apie nustatytus sąlytį turėjusius asmenis ir saugiai tvarkyti jų epidemiologiškai reikšmingus duomenis bei asmens duomenis valstybiniu ir teritoriniu lygiu, siekiant užkirsti kelią užkrečiamųjų ligų plitimui bei tinkamai valdyti ypatingąsias epidemines situacijas;

7.3. užtikrinti saugius duomenų mainus su kitomis nustatytomis informacinėmis sistemomis;

7.4. automatizuoti duomenų nustatytiems gavėjams teisės aktuose numatytoms funkcijoms vykdyti teikimą;

7.5. sudaryti technines galimybes atlikti operatyvią ir retrospektyvią epidemiologinę duomenų analizę bei statistinius skaičiavimus;

7.6. sudaryti technines galimybes apibendrinti ir realiu laiku skelbti visuomenei aktualią informaciją apie sergamumą užkrečiamosiomis ligomis, siekiant užkirsti kelią užkrečiamųjų ligų plitimui bei tinkamai valdyti ypatingąsias epidemines situacijas;

7.7. *Neteko galios nuo 2020-09-15*

Papunkčio naikinimas:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

7.8. sudaryti galimybę naudotojams nustatyti sąlytį turėjusius asmenis ir įspėti juos dėl galimos grėsmės užsikrėsti užkrečiama liga.

8. Pagrindinės Informacinės sistemos funkcijos:

8.1. rinkti ir kaupti ligonių, asmenų, turėjusių su jais sąlytį bei įtariamų, kad serga užkrečiamosiomis ligomis, užkrečiamųjų ligų epidemiologinei diagnostikai reikšmingus duomenis;

8.2. formuoti ir teikti visuomenei bei sergantiesiems užkrečiamosiomis ligomis informaciją apie susirgimo plitimą stabdančius veiksmus ir kitą naudingą informaciją;

8.3. nustatyti sąlytį su sergančiaisiais užkrečiamosiomis ligomis turėjusius asmenis ir informuoti į rizikos zoną patekusius asmenis;

8.4. atlikti duomenų analizes ir formuoti ataskaitas;

8.5. *Neteko galios nuo 2020-09-15*
Papunkčio naikinimas:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

8.6. administruoti ir identifikuoti Informacinės sistemos naudotojus

II SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINĖ STRUKTŪRA

9. Informacinės sistemos valdytojas ir tvarkytojas – Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (toliau – NVSC).
Punkto pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

10. Asmens duomenų valdytojas ir tvarkytojas – NVSC.
Punkto pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

11. Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas turi Įstatymo nustatytas teises ir pareigas, atlieka Įstatymo nustatytas funkcijas.

12. Informacinės sistemos asmens duomenų valdytojas ir tvarkytojas vykdo Reglamente (ES) 2016/679 nustatytas prievoles, turi šiame teisės akte nustatytas teises.

13. Informacinės sistemos tvarkytojas:

13.1. tvarko Informacinės sistemos duomenis (tarp jų – ir asmens duomenis) Nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Informacinės sistemos veiklą, nustatyta tvarka;
Papunkčio pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.2. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą;

13.3. vadovaudamasis Nuostatais, kitais teisės aktais, reglamentuojančiais Informacinės sistemos saugą, imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį – techninėmis ir organizacinėmis priemonėmis užtikrina Informacinės sistemos saugą, Informacinės sistemos tvarkomų asmens duomenų konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais;

13.4. užtikrina duomenų subjektų teisių, nustatytų Reglamento (ES) 2016/679 III skyriuje, įgyvendinimą pagal Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos valdomose informacinėse sistemose tvarkos aprašą, patvirtintą Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos direktoriaus 2023 m. kovo 13 d. įsakymu Nr. VKE-73 „Dėl Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos valdomose informacinėse sistemose tvarkos aprašo patvirtinimo
Papunkčio pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.5. Nuostatų, kitų teisės aktų, reglamentuojančių Informacinės sistemos veiklą, nustatyta tvarka užtikrina, kad būtų laikomasi Reglamento (ES) 2016/679 32–36 straipsniuose nustatytų prievolių, atsižvelgdamas į asmens duomenų tvarkymo pobūdį ir turimą informaciją
Papunkčio pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.6. užbaigus teikti su duomenų tvarkymu susijusias paslaugas, ištrina visus asmens duomenis ir jų kopijas, išskyrus atvejus, kai teisės aktuose reikalaujama asmens duomenis saugoti;
Papunkčio pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.7. *Neteko galios nuo 2023-08-26*
Papunkčio naikinimas:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.8. teikia pranešimus apie asmens duomenų saugumo pažeidimus asmens duomenų priežiūros institucijai ir duomenų subjektui bei atlieka kitas reikalingas asmens duomenų saugumo pažeidimų valdymo procedūras pagal Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašą, patvirtintą Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos direktoriaus 2019 m. gruodžio 30 d. įsakymu Nr. VKE-596 „Dėl Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo patvirtinimo
Papunkčio pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.9. sudaro ir pasirašo sutartis su duomenų teikėjais ir duomenų gavėjais;

13.10. koordinuoja ir administruoja Informacinės sistemos duomenų tvarkymą, keitimąsi duomenimis ir jų apskaitą;

13.11. administruoja Informacinės sistemos duomenų saugyklą, duomenų archyvą ir užtikrina jų saugą;

13.12. užtikrina Informacinės sistemos duomenų tvarkymo teisėtumą ir duomenų patikimumą;

13.13. laikosi Reglamento (ES) 2016/679 28 straipsnio 2 ir 4 dalyse nurodytų kito asmens duomenų tvarkytojo (toliau – subtvarkytojas) pasitelkimo sąlygų:

13.13.1. *Neteko galios nuo 2023-08-26*
Papunkčio naikinimas:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

13.13.2. subtvarkytojui taiko tokius pačius asmens duomenų apsaugos įsipareigojimus ir asmens duomenų saugumo reikalavimus, kokie nustatyti Informacinės sistemos asmens duomenų tvarkytojui, visų pirma, prievolė pakankamai užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus

įgyvendintos tokiu būdu, kad asmens duomenų tvarkymas atitiktų Reglamento (ES) 2016/679 32 straipsnio nusotatas;

13.13.3. kontroliuoja subtvarkytojo veiklą ir visiškai atsako už Nuostatų 13.13.2 papunktyje nurodytų subtvarkytojo prievolių nevykdymą;

13.14 atlieka kitas Nuostatuose ir kituose teisės aktuose, susijusiuose su Informacinės sistemos tvarkymu, nustatytas funkcijas.

14. Informacinės sistemos duomenų teikėjai:

14.1. Lietuvos Respublikos sveikatos apsaugos ministerija teikia Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenis (Registrų ir informacinių sistemų registro (toliau – RISR) kodas 2994);

14.2. VšĮ Kauno miesto greitosios medicinos pagalbos stotis teikia registracijos sistemoje Hybrid LAB tvarkomus duomenis;

14.3. Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos – informaciją apie asmenų, esančių izoliacijoje, patikrinimų rezultatus;

Papunkčio pakeitimai:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104
Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

14.4. Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos – Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos duomenis apie asmens sienos kirtimo datą (RISR kodas 9701);

Papunkčio pakeitimai:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

14.5. Europos Komisijos (toliau – Komisija) valdomas nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką užtikrinantis sietinis tinklų sietuvas.

Papildyta papunkčiu:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

III SKYRIUS
INFORMACINĖS SISTEMOS INFORMACINĖ STRUKTŪRA

15. Informacinėje sistemoje kaupiami šie duomenys:

15.1. Ligonio, asmens, įtariamo, kad serga, ir sąlytį turėjusių asmenų duomenys:

15.1.1. asmens informacija:

15.1.1.1. pavardė;

15.1.1.2. vardas;

15.1.1.3. gimimo data;

15.1.1.4. asmens kodas;

15.1.1.5. pilietybė;

15.1.1.6. lytis;

15.1.1.7. kalba;

15.1.1.8. profesija (kariškis / krovinio transporto vairuotojas / sveikatos priežiūros specialistas / policininkas / ugdymo įstaigos darbuotojas / kita);

15.1.1.9. darbovietė / mokymo įstaiga;

15.1.1.10. pirminė asmens sveikatos priežiūros įstaiga (poliklinika);

15.1.2. asmens kontaktinė informacija:

15.1.2.1. mobiliojo telefono ryšio numeris;

15.1.2.2. darbo telefono numeris;

15.1.2.3. namų telefono numeris;
15.1.2.4. kitas telefono numeris;
15.1.2.5. elektroninio pašto adresas;
15.1.3. sąlyčio informacija:
15.1.3.1. rizikos kategorija;
15.1.3.2. sąlyčio data;
15.1.3.3. sąlyčio tipas;
15.1.3.4. sąlyčio vieta / pobūdis;
15.1.3.5. jei registruojama šeima / grupė – šeimos / grupės pavadinimas;
15.1.3.6. šeimos / grupės informacija;
15.1.3.7. tretieji asmenys, su kuriais turėjo artimą sąlytį;
15.1.4. kelionės informacija:
15.1.4.1. atvykimo į Lietuvos Respubliką būdas;
15.1.4.2. oro linijų / vežėjo pavadinimas;
15.1.4.3. skrydžio / reiso numeris;
15.1.4.4. sėdėjimo vietos numeris;
15.1.4.5. atvykimo data;
15.1.4.6. šalis ar šalies vietovė, iš kur atvyko;
15.1.4.7. atvykimo vietos informacija;
15.1.4.8. išvykimo iš paveiktos teritorijos data;
15.1.4.9. laikas, planuojamas praleisti Lietuvoje;
15.1.4.10. persėdimo ar ilgesnio sustojimo vietos ir datos;
15.1.4.11. laikas, praleistas paveiktoje šalyje;
15.1.4.12. buvimą paveiktose šalyse faktą įrodantys dokumentai;
15.1.5. nuolatinės gyvenamosios vietos adresas (gatvės pavadinimas, namo numeris, buto numeris, miestas, savivaldybė, šalis, pašto kodas);
15.1.6. laikinosios gyvenamosios vietos adresas (viešbučio pavadinimas, gatvės pavadinimas, namo numeris, buto numeris, miestas, savivaldybė, šalis, pašto kodas);
15.1.7. šeimos informacija (nepilnamečių asmenų (iki 18 metų):
15.1.7.1. pavardė;
15.1.7.2. vardas;
15.1.7.3. sėdėjimo vietos numeris (jei keliavo);
15.1.7.4. amžius;
15.1.8. kontaktinė informacija apie asmenį, kuris galės susisiekti per 30 dienų (vardas, pavardė, miestas, šalis, mobiliojo telefono numeris, kitas telefono numeris, elektroninio pašto adresas);
15.1.9. stebėjimo statusas (asmuo stebimas / nestebimas);
15.1.10. kita informacija:
15.1.10.1. duomenys apie nedarbingumo pažymėjimo reikalingumą;
15.1.10.2. duomenys apie reikalingą izoliacijos galimybę;
15.1.10.3. duomenys apie reikalingą transportą pervežant;
15.1.10.4. izoliacijos režimo laikymosi periodas (data nuo–iki);
15.1.10.5. atsakingas NVSC departamentas;
15.1.10.6. NVSC departamento padalinys;
15.1.10.7. stebėseną vykdantis specialistas / savanoris;
15.1.10.8. stebėjimo statusas;
15.1.10.9. kito skambučio data;
15.1.10.10. sutikimas (sąlytį su užsikrėtusiu turėjusio asmens pateikta informacija apie jo sutikimą izoliuotis);

15.1.11. asmens stebėsenos informacija:
15.1.11.1. temperatūra;
15.1.11.2. jaučiami simptomai;
15.1.11.3. *Neteko galios nuo 2020-11-18*
Papunkčio naikinimas:
Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

15.1.11.4. socialinės pagalbos, psichologinės pagalbos reikalingumas;
15.1.11.5. asmens stebėjimo rezultatas;
15.1.11.6. asmuo patikrintas (taip / ne);
15.1.11.7. stebėsenos data;
15.1.11.8. patikrinęs skyrius (policija / skyrius);
15.1.11.9. ambulatorinio apsilankymo aprašymo E025 formos duomenys su TLK-10-AM kodu Z86.1 – buvusios asmeniui nepatikslintos infekcinės ir parazitinės ligos;
Papildyta papunkčiu:
Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

15.1.11.10. ambulatorinio apsilankymo aprašymo E025 formos duomenys su TLK-10-AM kodu Z29.0 – izoliacija.
Papildyta papunkčiu:
Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

15.1.12. mobiliosios programėlės duomenys:
15.1.12.1. artumo su kitais programėlės naudotojais duomenys (data, atstumas, trukmė, kito naudotojo programėlės raktas);
15.1.12.2. mobiliojo telefono numeris, kuriuo trumpąja telefono žinute siunčiamas susirgimui patvirtinti skirtas kodas;
15.1.12.3. paskelbimo susirgusiu patvirtinimo kodas;
15.1.12.4. užsikrėtusio asmens pseudoniminiai asmens duomenys (užsikrėtusiojo raktai, raktų kilmės šalis, raktų susijusios šalys, informacija apie infekcijos patvirtinimą).
Papunkčio pakeitimai:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

15.2. Kelionių duomenys:
15.2.1. Skrydžio, kelto identifikacinis numeris;
15.2.2. Oro linijų, kelto pavadinimas;
15.2.3. Skrydžio, kelto numeris;
15.2.4. Išvykimo vieta;
15.2.5. Atvykimo vieta;
15.2.6. Atvykimo data ir laikas;
15.2.7. Keleivių skaičius.
15.3. Laboratorinių tyrimų duomenys:
15.3.1. Tyrimo užsakymo duomenys;
15.3.2. Tyrimo atsakymo duomenys;
15.3.3. Tiriamojo asmens duomenys.
15.4. Informacinėje sistemoje tvarkomi Informacinės sistemos naudotojų duomenys:
15.4.1. Asmens kodas;
15.4.2. Vardas;
15.4.3. Pavardė;

15.4.4. Atstovaujama institucija;

15.4.5. Telefono numeris ir (arba) el. pašto adresas.

16. Duomenų teikėjai teikia šiuos duomenis:

16.1. iš Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos teikiami Nuostatų 15.1.11.9, 15.1.11.10 ir 15.3 papunkčiuose nurodyti duomenys;

Papunkčio pakeitimai:

Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

16.2. iš registracijos sistemos Hybrid LAB teikiami Nuostatų 15.1.2.1 ir 15.1.2.4 papunkčiuose nurodyti duomenys;

Papunkčio pakeitimai:

Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

16.3. iš Policijos atliktų asmenų, esančių izoliacijoje, patikrinimų teikiami Nuostatų 15.1.11.5 papunktyje nurodyti duomenys;

Papunkčio pakeitimai:

Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115

16.4. iš Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos teikiami Nuostatų 15.1.4.5 papunktyje nurodyti duomenys;

Papunkčio pakeitimai:

Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

16.5. iš Komisijos valdomo nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką užtikrinančio sietinio tinklų sietuvo teikiami Nuostatų 15.1.12.4 papunktyje nurodyti duomenys.

Papildyta papunkčiu:

Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

17. Už Nuostatų 15 punkte nurodytų duomenų, teikiamų į Informacinę sistemą, teisingumą, tikslumą ir pateikimą laiku įstatymų nustatyta tvarka atsako duomenų teikėjai.

IV SKYRIUS
INFORMACINĖS SISTEMOS FUNKCINĖ STRUKTŪRA

18. Informacinės sistemos funkcinę struktūrą sudaro:

18.1. naudotojų administravimo ir autentifikacijos posistemis, kurio funkcijos:

18.1.1. tvarkyti Informacinės sistemos duomenų naudotojus, jų teises ir roles;

18.1.2. vykdyti naudotojų prisijungimą prie Informacinės sistemos;

18.1.3. autentifikuoti naudotojus.

18.2. pranešimų posistemis, kurio funkcijos:

18.2.1. siųsti priminimus ir pranešimus;

18.2.2. informuoti apie gautus naujus ir patikslintus duomenis.

18.3. duomenų rinkimo posistemis, kurio funkcijos:

18.3.1. surinkti duomenis;

18.3.2. vykdyti duomenų pateikimą.

18.4. ataskaitų ir duomenų atvaizdavimo posistemis, kurio funkcijos yra:

18.4.1. formuoti sveikatos ir su ja susijusių duomenų ataskaitas.

18.4.2. siųsti duomenų ataskaitas adresatams;

18.4.3. atvaizduoti sukauptus duomenis įvairiomis formomis – lentelėmis, grafikais, žemėlapyje;

18.4.4. vykdyti duomenų paiešką bei filtruoti duomenis.

18.5. išorinio portalo turinio valdymo posistemis, kurio funkcijos:

18.5.1. publikuoti informaciją;

18.5.2. atlikti bendrines turinio valdymo funkcijas.

18.6. administravimo posistemis, kurio funkcijos:

18.6.1. saugoti ir kaupti informacinės sistemos atliktus veiksmus;

18.6.2. tvarkyti klasifikatorius.

18.7. duomenų mainų posistemis, kurio funkcijos:

18.7.1. importuoti iš duomenis duomenų teikėjų;

18.7.2. eksportuoti duomenis gavėjams.

18.8. Mobiliosios programėlės aptarnavimo posistemis, kurio funkcijos yra:

18.8.1. perduoti patvirtinimo kodą, suteiktą mobiliosios programėlės naudotojui, kuriam konstatuota užkrečiamoji liga;

18.8.2. priimti užsikrėtusių asmenų pseudoniminius duomenis (iš mobiliosios programėlės ir Europos Komisijos programėlių sąveiką užtikrinančio sietinio tinklų sietuvo);

18.8.3. perduoti užsikrėtusiųjų asmenų pseudoniminius duomenis (mobiliajai programėlei ir Europos Komisijos programėlių sąveiką užtikrinančiam sietiniam tinklų sietuvui);

18.8.4. priimti iš mobiliosios programėlės statistinius duomenis apie tai, kad mobiliosios programėlės naudotojas gavo įspėjimą apie sąlytį su užsikrėtusiu asmeniu.

Papunkčio pakeitimai:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

18.9. mobilioji programėlė, kurios funkcijos yra:

18.9.1. skleisti mobiliosios programėlės raktus, leidžiančius kitai programėlei stebėti artumą su raktus skleidžiančia programėle;

18.9.2. artumo su kitais mobiliosios programėlės naudotojais registravimas;

18.9.3. leisti mobiliosios programėlės naudotojui paskelbti apie užsikrėtimo užkrečiamąja liga faktą;

18.9.4. atsekti kontaktus ir įspėti mobiliosios programėlės naudotoją apie sąlytį su užsikrėtusiu asmeniu.

Papunkčio pakeitimai:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

18.10. duomenų archyvavimo posistemis, kurio funkcijos:

18.10.1. sudaryti statistinių duomenų archyvų bylas;

18.10.2. saugoti statistinių duomenų archyvų bylas.

V SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

19. Informacinės sistemos nuasmeninti apibendrinti duomenys yra vieši ir teikiami institucijoms, kitiems juridiniams ir fiziniams asmenims. Informacinėje sistemoje tvarkomi asmens duomenys teikiami ir naudojami vadovaujantis Reglamentu (ES) 2016/679, Nuostatais ir kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais.

20. Informacinės sistemos apibendrinti duomenys gali būti:

20.1. pateikiami peržiūrėti leidžiamosios kreipties būdu internetu;

20.2. perduodami automatiniu būdu;

20.3. pateikiami raštu, paštu, elektroniniu paštu ar kitomis elektroninio komunikavimo priemonėmis.

21. Informacinės sistemos duomenų gavėjai gautus duomenis ir informaciją gali naudoti tik tokiam tikslui, tokios apimties ir tokiu būdu, kaip nurodyta duomenų teikimo sutartyje arba prašyme. Informacinės sistemos duomenų gavėjas negali keisti iš Informacinės sistemos gautų duomenų ir informacijos ir juos naudodamas privalo nurodyti duomenų šaltinį.

22. Informacinės sistemos duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių fiziniams, judriniams asmenims, juridinio statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami vadovaujantis Įstatymu ir Reglamentu (ES)2016/679.

23. Kitų valstybių, išskyrus Europos Sąjungos valstybes nares ir Europos ekonominės erdvės valstybes, fiziniams, juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms duomenys teikiami, jeigu tai neprieštarauja Lietuvos Respublikos įstatymams, Reglamentui (ES) 2016/679, tarptautinėms sutartims, Europos Sąjungos teisės aktams ir kitiems norminiams teisės aktams.

24. Informacinės sistemos duomenis teikia Informacinės sistemos tvarkytojas. Duomenys teikiami tokio turinio ir tokios formos, kokie yra naudojami Informacinėje sistemoje, ir nereikalauja papildomo duomenų apdorojimo.

25. Daugkartinio teikimo atveju Informacinės sistemos asmens duomenys teikiami pagal Informacinės sistemos tvarkytojo ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį arba, kai teisės aktais yra nustatyta pareiga šiuos duomenis teikti.

25[1]. Komisijos valdomam nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką užtikrinančiam sietiniam tinklų sietuvui teikiami Nuostatų 15.1.12.4 papunktyje nurodyti duomenys.

Papildyta punktu:
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

26. Vienkartinio teikimo atveju Informacinės sistemos asmens duomenys teikiami pagal gavėjo prašymą pateiktą Informacinės sistemos tvarkytojui. Prašyme turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti duomenų apimtis.

27. Informacinės sistemos duomenys duomenų gavėjams teikiami neatlygintinai.

28. Kai atsisakoma teikti Informacinės sistemos tvarkomus duomenis, asmeniui, pateikusiam prašymą juos gauti, Informacinės sistemos tvarkytojas praneša apie priimtą sprendimą atsisakyti tenkinti asmens prašymą ir suteikia informaciją apie tokio sprendimo apskundimo tvarką.

29. Informacinės sistemos tvarkytojo sprendimai atsisakyti teikti Informacinės sistemos duomenis gali būti skundžiami Lietuvos Respublikos teisės aktų nustatyta tvarka.

30. Informacinės sistemos sudaryti dokumentų rinkiniai (stebėsenos statistinės ataskaitos), t. y. atviri duomenys, teikiami pakartotinai panaudoti bei publikuojami, vadovaujantis Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymo 19–21 straipsnių nuostatomis.

31. Duomenų gavėjai, duomenų subjektai, registro ar valstybės informacinės sistemos tvarkytojai, kiti asmenys turi teisę reikalauti ištaisyti netikslius duomenis. Gavęs šį reikalavimą, Informacinės sistemos tvarkytojas privalo per 5 darbo dienas nuo reikalavimo ir jame nurodytus faktus patvirtinančių dokumentų gavimo ištaisyti nurodytus netikslumus ir informuoti apie tai netikslius duomenis ištaisyti reikalavusį asmenį.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

33. Informacinės sistemos duomenų saugą reglamentuoja Informacinės sistemos valdytojo

tvirtinami Informacinės sistemos duomenų saugos nuostatai ir kiti saugos politiką įgyvendinantys dokumentai, kurie rengiami, derinami ir tvirtinami teisės aktų nustatyta tvarka. Siekiant užtikrinti Informacinės sistemos duomenų saugą, vadovaujamasi:

33.1. Reglamentu (ES) 2016/679;

33.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

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

33.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

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

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

34. Už Informacinės sistemos duomenų saugą atsako Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas teisės aktų nustatyta tvarka.

35. Duomenys Informacinėje sistemoje saugomi iki ypatingosios epidemiologinės situacijos pabaigos, bet ne ilgiau nei 1 metus. Mobiliosios programėlės tvarkomi artumo ir užsikrėtusių asmenų pseudoniminiai asmens duomenys saugomi 14 dienų. Pasibaigus Informacinės sistemos duomenų saugojimo laikui, Informacinės sistemos duomenys yra perduodami Lietuvos vyriausiojo archyvaro tarnybai arba sunaikinami Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

Punkto pakeitimai:

Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104

36. Asmenys, kurie tvarko asmens duomenis, įpareigojami saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja jiems pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas, pasibaigus jų darbo ar sutartiniams santykiams.

VII SKYRIUS
INFORMACINĖS SISTEMOS FINANSAVIMAS

37. Informacinės sistemos kūrimas ir plėtra finansuojami Lietuvos Respublikos valstybės biudžeto, įskaitant Europos Sąjungos fondus, lėšomis. Informacinės sistemos eksploatacija ir palaikymas finansuojami Lietuvos Respublikos valstybės biudžeto lėšomis bei gali būti apmokami iš kitų teisėtų finansavimo šaltinių.

VIII SKYRIUS
INFORMACINĖS SISTEMOS MODERNIZAVIMAS IR LIKVIDAVIMAS

38. Informacinė sistema modernizuojama arba likviduojama Įstatymo ir Aprašo nustatyta tvarka.

39. Likviduojamos Informacinės sistemos duomenys perduodami kitai informacinei sistemai, sunaikinami arba perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

40. Asmenys, pažeidę Nuostatų ir kitų teisės aktų nuostatas, reglamentuojančias Informacinės sistemos veiklą, atsako įstatymų nustatyta tvarka.

41. Duomenų subjekto teisių, įtvirtintų Reglamente (ES) 2016/679, įgyvendinimo tvarką nustato Informacinės sistemos valdytojas.

_____

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2020 m. gegužės 5 d. įsakymu Nr. V-1067

UŽKREČIAMŲJŲ LIGŲ, GALINČIŲ IŠPLISTI IR KELTI GRĖSMĘ, STEBĖSENOS IR KONTROLĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. Informacinės sistemos elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Informacinė sistemos elektroninę informaciją, užtikrinti Informacinė sistemos elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą, vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevenciją.

3. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 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), Lietuvos standartuose LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

4. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

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

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

4.3. Informacinės sistemos tvarkymo kontrolė;

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

4.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;

4.6. Informacinės sistemos veiklos tęstinumo užtikrinimas.

5. Saugos nuostatai taikomi Informacinės sistemos valdytojui ir tvarkytojui bei asmens duomenų valdytojui ir tvarkytojui – Nacionaliniam visuomenės sveikatos centrui prie Lietuvos

Respublikos sveikatos apsaugos ministerijos (Kalvarijų g. 153, LT-08352, Vilnius), Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriui, Informacinės sistemos naudotojams.

Punkto pakeitimai:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

6. Informacinės sistemos valdytojas atlieka Informacinės sistemos nuostatuose nustatytas funkcijas, taip pat:

6.1. tvirtina Saugos nuostatus ir Informacinės sistemos saugos politiką įgyvendinančius dokumentus (toliau – Informacinės sistemos saugos dokumentai);

6.2. atlieka kitas Saugos nuostatuose ir elektroninės informacijos saugą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

7. Informacinės sistemos tvarkytojas:

7.1. pagal kompetenciją atsako už Informacinės sistemos elektroninės informacijos tvarkymo teisėtumą ir saugą;

7.2. užtikrina tinkamų organizacinių ir techninių priemonių, skirtų elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, įgyvendinimą;

7.3. pagal kompetenciją vykdo reikalavimus, nustatytus Informacinės sistemos saugos dokumentuose;

7.4. *Neteko galios nuo 2023-08-26*

Papunkčio naikinimas:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

7.5. užtikrina, kad Informacinės sistemos naudotojai, turintys teisę naudotis Informacinės sistemos elektronine informacija, laikytųsi reikalavimų, nustatytų Saugos nuostatuose ir Informacinės sistemos saugos dokumentuose;

7.6. atlieka Informacinės sistemos duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Informacinės sistemos veikimą;

7.7. užtikrina saugią Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.8. *Neteko galios nuo 2023-08-26*

Papunkčio naikinimas:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

7.9. skiria Informacinės sistemos duomenų valdymo įgaliotinį, Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorių;

7.10. *Neteko galios nuo 2023-08-26*

Papunkčio naikinimas:
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741

8. Informacinės sistemos saugos įgaliotinis:

8.1. teikia Informacinės sistemos tvarkytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

8.2. teikia Informacinės sistemos tvarkytojo vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;

8.3. koordinuoja saugos incidentų, įvykusių Informacinėje sistemoje, tyrimą;

8.4. organizuoja Informacinės sistemos rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą;

8.5. duoda Informacinės sistemos tvarkytojo naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Informacinės sistemos saugos politikos įgyvendinimu;

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

8.7. atlieka kitas Informacinės sistemos tvarkytojo vadovo pavestas ir Informacinės sistemos saugos dokumentuose jam priskirtas funkcijas.

9. Informacinės sistemos administratoriaus funkcijos:

9.1. užtikrina Informacinės sistemos techninės ir programinės įrangos įdiegimą ir funkcionavimą;

9.2. diegia ir prižiūri programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

9.3. suteikia teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

9.4. užtikrina 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 nustato Informacinės sistemos pažeidžiamas vietas;

9.5. pagal kompetenciją dalyvauja, vykdant saugumo reikalavimų įgyvendinimo stebėseną;

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

9.7. informuoja Informacinės sistemos saugos įgaliotinį apie saugos incidentus ir teikia siūlymus dėl saugos incidentų pašalinimo;

9.8. atsako už Informacinės sistemos duomenų bazės atsarginių kopijų darymą ir archyve esančių kopijų saugojimą;

9.9. atlieka kitas Informacinės sistemos tvarkytojo vadovo, saugos įgaliotinio pavestas ir Informacinės sistemos saugos dokumentuose jam nustatytas funkcijas.

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

10.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

10.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

10.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

10.4. 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);

10.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Saugos dokumentų turinio gairių aprašas ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtinti 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“;

10.6. 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“;

10.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti 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“;

10.8. 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“;

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

10.10. Informacinės sistemos saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. 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 – Elektroninės informacijos svarbos nustatymo gairių aprašas), 9.1 ir 9.2 papunkčiais, Informacinės sistemos tvarkoma informacija priskiriama prie vidutinės svarbos informacijos kategorijos.

12. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12.3 papunkčiu, Informacinė sistema priskiriama prie trečiosios kategorijos informacinių sistemų – Informacinėje sistemoje tvarkoma vidutinės svarbos informacija.

13. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą 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 šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas.

14. 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:

14.1. 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);

14.2. 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);

14.3. 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.

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

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

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

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

16. 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.

17. Informacinės sistemos rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama Informacinės sistemos tvarkytojo vadovui.

18. Elektroninės informacijos saugos priemonių parinkimo principai:

18.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

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

18.4. Informacinės sistemos veiklos tęstinumas ir elektroninės informacijos sauga turi būti užtikrinama patiriant kuo mažiau išlaidų.

19. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę kartą per metus organizuojamas informacinių technologijų saugos atitikties vertinimas.

20. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Informacinės sistemos tvarkytojo vadovui.

21. Informacinės sistemos rizikos įvertinimo ataskaitos, Informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, 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 LR krašto apsaugos ministro 2018 m. gruodžio 10 d. įsakymu Nr. V-1183, nustatyta tvarka.

III SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

22. 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:

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

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

22.3. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 16 valandų.

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

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

23.2. programinė įranga turi būti nuolatos atnaujinama, laikantis gamintojo reikalavimų;

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

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

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

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

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

24.2. 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;

24.3. 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.

25. Leistinos kompiuterių naudojimo ribos:

25.1. 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;

25.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti naudojamas įjungimo slaptažodis;

25.3. Informacinės sistemos naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo, duomenys, susiję su Informacine sistemaa, nešiojamuose kompiuteriuose turi būti šifruojami.

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

26.1. 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;

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

26.3. 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;

26.4. 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.

27. Informacinės sistemos atsarginės duomenų bazės kopijos daromos automatiniu būdu kiekvieną dieną, esant aktyviai Informacinės sistemos duomenų bazei. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Prireikus jas atkurti turi teisę tik Informacinės sistemos administratorius ar jį pavaduojantis asmuo. Kopijų darymo ir saugojimo tvarka nustatoma Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

28. Duomenys apie Informacinės sistemos naudotojų, Informacinės sistemos administratoriaus atliktus veiksmus su Informacinės sistemos elektronine informacija saugomi ne trumpiau nei vienus metus.

29. Informacinės sistemos saugomi duomenys yra šifruojami. Saugojimo ir šifravimo algoritmai privalo būti ne žemesni už AES256.

30. Duomenų teikimas į Informacinę sistemą privalo būti vykdomas naudojant saugų šifruotą kanalą TLS 1.2.

31. Informacinei sistemai galioja 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“ ir Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų, patvirtintų 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“ reikalavimai, nustatyti III kategorijos informacinei sistemai.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

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

33. Informacinės sistemos saugos įgaliotinis turi:

33.1. išmanyti elektroninės informacijos saugos užtikrinimo principus;

33.2. tobulinti kvalifikaciją elektroninės informacijos saugos srityje;

33.3. savo darbe vadovautis Saugos nuostatais ir Informacinės sistemos saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

34. Informacinės sistemos administratorius turi:

34.1. išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą;

34.2. mokėti administruoti ir prižiūrėti duomenų bazes;

34.3. būti susipažinęs su Informacinės sistemos nuostatais, Saugos nuostatais, Informacinės sistemos saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

35. Informacinės sistemos naudotojai turi:

35.1. turėti pagrindinius darbo kompiuteriu įgūdžius;

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

35.3. būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

36. Informacinės sistemos naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti Informacinės sistemos saugos įgaliotiniui.

37. Informacinės sistemos elektroninę informaciją tvarkyti gali asmenys, turintys pagrindinius darbo kompiuteriu įgūdžius, mokantys tvarkyti Informacinės sistemos elektroninę informaciją, nurodytą Informacinės sistemos nuostatuose ir susipažinę su Saugos nuostatų ir Informacinės sistemos saugos dokumentų reikalavimais.

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

38.1. 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.);

38.2. 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;

38.3. 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.);

38.4. 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;

38.5. 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.

39. 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

40. Informacinės sistemos naudotojus su Saugos nuostatais ir Informacinės sistemos 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.

41. Pakartotinai su Informacinės sistemos saugos dokumentais Informacinės sistemos naudotojai supažindinami jiems pasikeitus.

42. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Informacinės sistemos tvarkytojo Dokumentų valdymo sistemoje.

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

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. 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.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-2025, 2020-09-11, paskelbta TAR 2020-09-11, i. k. 2020-19104
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymo Nr. V-1067 „Dėl Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos steigimo ir jos nuostatų bei duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-2631, 2020-11-17, paskelbta TAR 2020-11-17, i. k. 2020-24115
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymo Nr. V-1067 „Dėl Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos steigimo ir jos nuostatų bei duomenų saugos nuostatų patvirtinimo“ pakeitimo

3.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-939, 2023-08-25, paskelbta TAR 2023-08-25, i. k. 2023-16741
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymo Nr. V-1067 „Dėl Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos steigimo ir jos nuostatų bei duomenų saugos nuostatų patvirtinimo“ pakeitimo