LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2018 M. SPALIO 2 D. ĮSAKYMO NR. V-1065 „DĖL VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ, VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ IR VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO“ PAKEITIMO

2020 m. lapkričio 26 d. Nr. V-2743

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. spalio 2 d. įsakymą Nr. V-1065 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos naudotojų administravimo taisyklių, Visuomenės sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių ir Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“:

1. Pakeičiu preambulę ir ją išdėstau taip:

„Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi 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“, 8 punktu, 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 ir 6 punktais:“.

2. Pakeičiu nurodytu įsakymu patvirtintas Visuomenės sveikatos stebėsenos informacinės sistemos naudotojų administravimo taisykles ir jas išdėstau nauja redakcija (pridedama).

3. Pakeičiu nurodytu įsakymu patvirtintas Visuomenės sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles ir jas išdėstau nauja redakcija (pridedama).

4. Pakeičiu nurodytu įsakymu patvirtintą Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo planą ir jį išdėstau nauja redakcija (pridedama).

Laikinai einantis sveikatos apsaugos ministro pareigas Aurelijus Veryga

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2020 m. lapkričio 18 d. raštu Nr. (4.1) 6K-720

Parengė
R. Jankauskas
2020-11-

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2018 m. spalio 2 d.
įsakymu Nr. V-1065
(Lietuvos Respublikos sveikatos apsaugos
ministro 2020 m. lapkričio d. 26
įsakymo Nr. V-2743
redakcija)

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Visuomenės sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) naudotojų administravimo taisyklės (toliau – Taisyklės) taikomos visiems Informacinės sistemos naudotojams, Informacinės sistemos administratoriui ir saugos įgaliotiniui.

2. Prieigos prie Informacinės sistemos elektroninės informacijos suteikimo principai:

2.1. „būtina darbui“ – Informacinės sistemos naudotojams gali būti suteikta prieigos teisė tik prie tokios apimties duomenų, kokios reikia jo numatytoms funkcijoms atlikti;

2.2. „būtina žinoti“ – prieigos teisė prie duomenų gali būti suteikta tik atitinkamą leidimą dirbti ar susipažinti su šiais duomenimis turintiems asmenims.

II SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ IR ADMINISTRATORIAUS ĮGALIOJIMAI, TEISĖS IR PAREIGOS

3. Prieš tapdamas Informacinės sistemos naudotoju, darbuotojas privalo susipažinti su 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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), Informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. įsakymu Nr. V-405 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos duomenų saugos nuostatai), ir saugos politiką įgyvendinančiais dokumentais (toliau visi kartu – saugos dokumentai) ir saugoti Informacinėje sistemoje tvarkomų naudotojų asmens duomenų paslaptį. Kiekvienas Informacinės sistemos naudotojas pasirašo Taisyklių priede nustatytos formos pasižadėjimą saugoti Visuomenės sveikatos stebėsenos informacinėje sistemoje tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų (toliau – pasižadėjimas). Kiekvienas Informacinės sistemos tvarkytojas saugo savo įstaigos Informacinės sistemos naudotojų pasirašytus pasižadėjimus.

4. Informacinės sistemos naudotojai:

4.1. turi teisę rinkti, tvarkyti, perduoti, saugoti ar kitaip naudoti Informacinės sistemos elektroninę informaciją tik atlikdami savo tiesiogines funkcijas;

4.2. turi teisę naudotis tik tomis funkcijomis (duomenų paieška, peržiūra, įvedimas, koregavimas, taisymas, keitimas ir kt.) ir duomenimis, prie kurių prieigą jiems suteikė Informacinės sistemos administratorius;

4.3. privalo užtikrinti jų naudojamų Informacinėje sistemoje tvarkomų duomenų konfidencialumą ir vientisumą, savo veiksmais netrikdyti Informacinės sistemos duomenų prieinamumo;

4.4. turi teisę teikti siūlymus dėl papildomų elektroninės informacijos saugos priemonių taikymo;

4.5. privalo laikytis saugos dokumentuose nustatytų reikalavimų, pastebėję Informacinės sistemos sutrikimus, neįprastą jos veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų naudotojų nederamus veiksmus, nedelsiant pranešti Informacinės sistemos administratoriui arba saugos įgaliotiniui;

4.6. baigę darbą ar pasitraukdami iš darbo vietos turi imtis priemonių, kad su informacija, kuri tvarkoma Informacinėje sistemoje, negalėtų susipažinti pašaliniai asmenys: atsijungti nuo Informacinės sistemos;

4.7. vykdyti kitas Informacinės sistemos naudotojų teises ir pareigas, nurodytas Informacinės sistemos saugos dokumentuose.

5. Informacinės sistemos administratorius vykdo Informacinės sistemos tarnybinių stočių, duomenų bazių ir Informacinės sistemos naudotojų administravimą. Jo įgaliojimai, teisės ir pareigos:

5.1. naudotojams suteikti, apriboti ar panaikinti prieigą prie Informacinės sistemos, keisti prieigos lygius;

5.2. užtikrinti, kad Informacinėje sistemoje nebūtų atliekami veiksmai, kurie gali sukelti bet kokio pobūdžio elektroninės informacijos saugos incidentą (neteisėtas Informacinės sistemos naudojimas, neteisėtas Informacinės sistemos elektroninės informacijos ir programinės įrangos kopijavimas ir kt.);

5.3. atsakyti už atsarginių Informacinės sistemos elektroninės informacijos kopijų darymą ir elektroninės informacijos atkūrimą duomenų praradimo atveju;

5.4. pagal pasirinktus paieškos kriterijus atlikti užklausas Informacinėje sistemoje, keisti naudotojų teises ir kt.;

5.5. diegti naujas duomenų bazės valdymo sistemos versijas, prižiūrėti Informacinės sistemos duomenų bazę;

5.6. diegti tarnybinių stočių programinės įrangos atnaujinimus;

5.7. administruoti Informacinės sistemos tarnybines stotis;

5.8. jungiantis prie Informacinės sistemos savo tapatybę patvirtinti slaptažodžiu arba kita tapatumo patvirtinimo priemone;

5.9. vykdyti kitas Informacinės sistemos administratoriaus ir naudotojų teises ir pareigas, nurodytas Informacinės sistemos duomenų saugos nuostatuose.

6. Informacinės sistemos administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms Informacinės sistemos naudotojo funkcijoms atlikti.

III SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

7. Informacinės sistemos naudotojų registravimo ir išregistravimo tvarka:

7.1. Informacinės sistemos administratorius, gavęs asmens, turinčio teisinį pagrindą tvarkyti Informacinės sistemos duomenis, prašymą, kuriame nurodyti Informacinės sistemos naudotojo duomenys: vardas, pavardė, elektroninio pašto adresas, telefono numeris, ir (ar) asmens kodas, institucijos juridinio asmens kodas ir pavadinimas, reikiamų teisių sąrašas, įregistruoja Informacinės sistemos pagrindinio tvarkytojo ir (ar) kito Informacinės sistemos tvarkytojo atsakingą asmenį (toliau – atsakingas asmuo), jei Informacinės sistemos tvarkytojas nurodo, kad jos įstaigos naudotojų registravimą (įregistravimą ir išregistravimą) atliks atsakingas asmuo. Atsakingas asmuo turi teisę registruoti (įregistruoti ir išregistruoti) tik tuos Informacinės sistemos naudotojus, kurie dirba toje pačioje įstaigoje;

7.2. Informacinės sistemos tvarkytojo atsakingas asmuo, gavęs asmens, turinčio teisinį pagrindą tvarkyti Informacinės sistemos duomenis, prašymą, kuriame nurodyti Informacinės

sistemos naudotojo duomenys: vardas, pavardė, pareigos, elektroninio pašto adresas, telefono numeris, ir (ar) asmens kodą, įregistruoja Informacinės sistemos tvarkytojo naudotojus, kurie tiesiogiai tvarko Informacinės sistemos duomenis;

7.3. pagrindinio Informacinės sistemos tvarkytojo naudotojai, atsakingi už Informacinės sistemos duomenų koordinavimą, registruoja Informacinės sistemos tvarkytojų naudotojus, jeigu Informacinės sistemos tvarkytojas neinformuoja Informacinės sistemos pagrindinį tvarkytoją apie tai, kad Informacinės sistemos tvarkytojo atsakingas asmuo atliks naudotojų registravimą;

7.4. gavęs suteiktą slaptažodį ir pirmą kartą prisijungęs prie Informacinės sistemos duomenų bazės, Informacinės sistemos naudotojas turi susipažinti su Visuomenės sveikatos stebėsenos informacinės sistemos nuostatais, patvirtintais Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. įsakymu Nr. V-405 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“, ir Informacinės sistemos duomenų saugos nuostatais ir patvirtinęs susipažinimo faktą, pirminį slaptažodį privalo nedelsdamas pakeisti nauju;

7.5. kiekvienas Informacinės sistemos naudotojas privalo naudoti tik jam suteiktą naudotojo vardą, saugoti slaptažodį ir jo neatskleisti tretiesiems (neįgaliotiems) asmenims;

7.6. Informacinės sistemos naudotojų duomenys registruojami ir kaupiami Informacinės sistemos duomenų bazėje.

8. Slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai:

8.1. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (didžiosios ir mažosios raidės, skaičiai, specialieji simboliai);

8.2. slaptažodžiui sudaryti neturi būti naudojama asmeninio pobūdžio (pavyzdžiui gimimo data, šeimos narių vardai, prisijungimo vardas, gyvenamosios vietos adresas ar jo sudėtinės dalys, telefono numeris ir kt.) informacija;

8.3. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;

8.4. nustatytas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius (5 kartai). Penkis kartus neteisingai įvedus slaptažodį, Informacinė sistema turi užsirakinti ir neleisti Informacinės sistemos naudotojui identifikuotis 15 minučių;

8.5. slaptažodis turi būti keičiamas kas 3 mėnesius, Informacinės sistemos naudotojo teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;

8.6. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, Informacinės sistemos naudotojas turi nedelsdamas jį pakeisti;

8.7. Informacinės sistemos naudotojui pamiršus slaptažodį, jis gali atsisiųsti per prisijungimo langą laikiną prisijungimo slaptažodį arba prisijungti prie Informacinės sistemos naudodamasis Valstybės informacinių išteklių sąveikumo platformos teikiamomis paslaugomis;

8.8. pirmojo prisijungimo prie Informacinės sistemos metu iš Informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

8.9. keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

8.10. papildomi reikalavimai Informacinės sistemos administratoriaus slaptažodžiams:

8.10.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

8.10.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

8.10.3. keičiant slaptažodį Informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

8.10.4. draudžiama Informacinės sistemos techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus;

8.11. draudžiama slaptažodžius atskleisti kitiems asmenims.

9. Informacinės sistemos naudotojų teisių dirbti su Informacinės sistemos duomenimis ribojimas ir (arba) naikinimas:

9.1. pasibaigus darbo santykiams, Informacinės sistemos naudotojo teisė naudotis Informacine sistema panaikinama. Informacinės sistemos naudotojo paskyrą panaikina asmuo, kuris

ją įregistravo. Informacinės sistemos naudotojas privalo ne vėliau kaip paskutinę savo darbo dieną informuoti asmenį, sukūrusį jo naudotojo paskyrą, apie savo darbo santykių pasibaigimą;

9.2. teisė dirbti su Informacinės sistemos duomenimis sustabdoma, kai Informacinės sistemos naudotojas nesinaudoja informacine sistema ilgiau kaip 18 mėnesių. Informacinės sistemos naudotojo paskyrą sustabdo asmuo, kuris ją įregistravo;

9.3. kai įstatymų nustatytais atvejais vidinis informacinės sistemos naudotojas nušalinamas nuo darbo (pareigų), netekus funkcijos tvarkyti Informacinės sistemos duomenų, pasibaigus tarnybos (darbo) santykiams, Informacinės sistemos naudotojo teisė naudotis informacine sistema panaikinama nedelsiant. Informacinės sistemos naudotojo paskyrą panaikina asmuo, kuris ją įregistravo.

10. Informacinėje sistemoje vykdoma Informacinės sistemos naudotojų paskyrų kontrolė:

10.1. kai Informacinės sistemos naudotojas nesinaudoja Informacine sistema ilgiau nei 18 mėnesių, jo paskyros galiojimas sustabdomas. Informacinės sistemos naudotojo paskyrų sustabdymo kontrolę vykdo Informacinės sistemos administratorius, o Informacinės sistemos administratoriaus sukurtų paskyrų sustabdymo kontrolę vykdo Informacinės sistemos saugos įgaliotinis;

10.2. pasikeitus Informacinės sistemos naudotojo veiklos pobūdžiui (perkėlus jį į kitas pareigas ir pan.), pasibaigus jo darbo santykiams, Informacinės sistemos naudotojo paskyra panaikinama nedelsiant, tačiau ne vėliau kaip paskutinę jo darbo dieną įstaigoje. Informacinės sistemos naudotojo paskyrų panaikinimo kontrolę vykdo Informacinės sistemos administratorius.

11. Informacinėje sistemoje vykdoma Informacinės sistemos administratoriaus paskyrų kontrolė:

11.1. Informacinės sistemos administratoriaus funkcijos atliekamos naudojant atskirą tam skirtą paskyrą, kuri nenaudojama kasdienėms Informacinės sistemos naudotojo funkcijoms atlikti;

11.2. nereikalinga ar nenaudojama Informacinės sistemos administratoriaus paskyra blokuojama nedelsiant ir ištrinama praėjus audito duomenų nustatytam saugojimo terminui.

12. Informacinės sistemos tvarkytojas turi parengti asmenų, kuriems suteiktos Informacinės sistemos administratoriaus teisės prisijungti prie Informacinės sistemos, sąrašą. Šis sąrašas periodiškai peržiūrimas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais Informacinės sistemos administratorius nušalinamas nuo darbo (pareigų).

_____

Visuomenės sveikatos stebėsenos
informacinės sistemos naudotojų
administravimo taisyklių
priedas

PASIŽADĖJIMAS
SAUGOTI VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖJE SISTEMOJE TVARKOMŲ ASMENS IR KITŲ DUOMENŲ PASLAPTĮ, LAIKYTIS DUOMENŲ SAUGOS REIKALAVIMŲ

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

1. Aš suprantu, kad:

1.1. savo darbe susipažinsiu su konfidencialia informacija, kuri negali būti atskleista ar perduota neįgaliotiems asmenims ar institucijoms;

1.2. draudžiama perduoti neįgaliotiems asmenims slaptažodžius ir kitus duomenis, leidžiančius naudojantis programinėmis ar techninėmis priemonėmis sužinoti konfidencialią informaciją, arba kitaip sudaryti sąlygas susipažinti su tokia informacija;

1.3. informacijos skleidimu laikomas ne tik duomenų perdavimas, bet ir sąlygų sudarymas neįgaliotiems asmenims gauti informaciją;

1.4. netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę pagal Reglamentą (ES) 2016/679, Lietuvos Respublikos įstatymus.

2. Man išaiškinta, kad konfidencialią informaciją pagal šį pasižadėjimą sudaro:

2.1. asmens duomenys suprantami, kaip apibrėžti Reglamente (ES) 2016/679 ;

2.2. informacija, kurią darbo metu patikėta tvarkyti ar naudotis, išskyrus, kai tokią informaciją teikti įpareigoja teisės aktai ar kompetentingos institucijos;

2.3. žinios apie Informacinėje sistemoje esančius kompiuterius, kompiuterinės įrangos sistemas, kompiuteriuose sukaupta informacija, apsaugos ir signalizacijos informacija.

3. Konfidencialia informacija nelaikoma tokia informacija, kuri:

3.1. jau yra žinoma informacijos gavėjui, jei dėl jos nėra konfidencialumo susitarimų su informacijos teikėju bei nėra kitaip informacijos teikėjui ar kitiems asmenims prisiimta neatskleidimo įsipareigojimų;

3.2. tampa informacijos gavėjui prieinama nesant konfidencialumo įsipareigojimų iš šaltinio, kuris nėra informacijos teikėjas ar bet kurio iš jų atstovas ir kuris, informacijos gavėjo žiniomis, nėra susaistytas konfidencialumo sutartimi ar kitaip įsipareigojęs informacijos teikėjui ar bet kurio iš jų atstovams;

3.3. jau yra viešai prieinama ne dėl informacijos gavėjo neteisėto atskleidimo arba yra vieša pagal teisės aktus.

4. Aš įsipareigoju:

4.1. saugoti konfidencialią informaciją;

4.2. tvarkyti konfidencialią informaciją vadovaudamasis Reglamentu (ES) 2016/679, Lietuvos Respublikos įstatymais ir kitais teisės aktais;

4.3. neatskleisti, neperduoti ir nesudaryti sąlygų įvairiomis priemonėmis susipažinti su tvarkoma informacija nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek Informacinėje sistemoje, tiek už jos ribų;

4.4. pranešti savo tiesioginiam vadovui arba asmeniui, atsakingam už informacijos saugumą, apie bet kokius bandymus sužinoti man patikėtą konfidencialią informaciją ir apie bet kokią situaciją, kuri gali kelti grėsmę informacijos saugumui;

4.5. pasibaigus darbo santykiams ar pasikeitus pareigoms, toliau saugoti darbo metu sužinotą konfidencialią informaciją.

5. Aš žinau, kad:

5.1. už konfidencialumo pasižadėjimo nesilaikymą bei kitų teisės aktų, reglamentuojančių konfidencialios informacijos tvarkymą, pažeidimus pagal Lietuvos Respublikos įstatymus kyla drausminė, tarnybinė, civilinė, administracinė arba baudžiamoji atsakomybė;

5.2. asmuo, patyręs žalą dėl neteisėto konfidencialios informacijos tvarkymo ar kitų duomenų tvarkytojo neteisėtų veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą;

5.3. institucija, atlyginusi žalą, patirtą nuostolį išsireikalauja įstatymų nustatyta tvarka iš informaciją tvarkančio darbuotojo, dėl kurio kaltės atsirado žala;

5.4. šis pasižadėjimas galios visą mano darbo laiką šioje įstaigoje, perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams.

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

_____
(data)

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. spalio 2 d.
įsakymu Nr. V-1065
(Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. lapkričio d. 26
įsakymo Nr. V-2743 redakcija)

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Visuomenės sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Informacijos tvarkymo taisyklės) tikslas – sudaryti sąlygas saugiai tvarkyti Visuomenės sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) elektroninę informaciją ir užtikrinti kibernetinį saugumą.

2. Informacinės sistemos duomenų bazėje tvarkomi Informacinės sistemos duomenys, nurodyti Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. įsakymu Nr. V-405 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos nuostatai), 16 punkte. Informacinėje sistemoje tvarkomi naudotojų asmens duomenys, kurie nurodyti Informacinės sistemos nuostatų 17 punkte.

3. 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“, 12.3 papunkčiu, Informacinėje sistemoje tvarkoma elektroninė informacija yra priskiriama vidutinės svarbos informacijos kategorijai, o informacinė sistema priskiriama trečiajai informacinių sistemų kategorijai.

4. Informacijos tvarkymo taisyklės privalomos Informacinės sistemos valdytojui, Informacinės sistemos tvarkytojams, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui bei saugos įgaliotiniui. Už Informacijos tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsako Informacinės sistemos saugos įgaliotinis. Už Informacinės sistemos elektroninės informacijos tvarkymą atsakingi:

4.1. Informacinės sistemos naudotojai, dirbantys Higienos institute, – už duomenų, nurodytų Informacinės sistemos nuostatų 16 ir 17 punktuose, tvarkymą;

4.2. Informacinės sistemos naudotojai:

4.2.1. asmens sveikatos priežiūros įstaigos – už duomenų, nurodytų Informacinės sistemos nuostatų 16.1, 16.3, 16.5 papunkčiuose, 17 punkte, tvarkymą;

4.2.2. visuomenės sveikatos priežiūros įstaigos ir Sveikatos apsaugos ministerijai pavaldžios biudžetinės įstaigos – už duomenų, nurodytų Informacinės sistemos nuostatų 16.5 papunktyje ir 17 punkte, tvarkymą;

4.2.3. stacionarines asmens sveikatos priežiūros paslaugas teikiančios įstaigos – už duomenų, nurodytų Informacinės sistemos nuostatų 16.2 papunktyje ir 17 punkte, tvarkymą;

4.2.4. savivaldybių visuomenės sveikatos biurai – už duomenų, nurodytų Informacinės sistemos nuostatų 16.4 papunktyje ir 17 punkte, tvarkymą;

4.3. Informacinės sistemos administratorius – už duomenų, nurodytų Informacinės sistemos nuostatų 16 ir 17 punktuose, tvarkymą, už Informacinės sistemos administravimą, duomenų bazių atkūrimą ir priežiūrą, prieinamumo užtikrinimą, klasifikatorių tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Kompiuterinės įrangos saugos priemonės turi atitikti šiuos reikalavimus:

5.1. Informacinės sistemos tarnybinės stotys turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį Informacinės sistemos tarnybinių stočių veikimą ne mažiau kaip 30 minučių;

5.2. Informacinės sistemos tarnybinėse stotyse ir Informacinės sistemos tvarkytojų kompiuterizuotose darbo vietose turi būti įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti;

5.3. apsaugai naudojama programinė įranga turi automatiškai elektroniniu paštu informuoti Informacinės sistemos administratorių apie Informacinės sistemos pagrindinio tvarkytojo naudotojų kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 12 valandų;

5.4. Informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei 16 valandų;

5.5. Informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

5.6. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

5.7. patekimas prie Informacinės sistemos pagrindinio tvarkytojo naudotojų darbo vietų turi būti kontroliuojamas: kompiuteriais, turinčiais prieigą prie Informacinės sistemos, galima naudotis tik Informacinės sistemos tvarkytojo patalpose;

5.8. prieiga prie Informacinės sistemos tarnybinių stočių turi būti kontroliuojama prieigos teises suteikiant tik Informacinės sistemos administratoriui arba kitam įgaliotam asmeniui;

5.9. prieiga prie Informacinės sistemos virtualių mašinų yra kontroliuojama prieigos teises suteikiant tik Informacinės sistemos administratoriui arba kitam įgaliotam asmeniui;

5.10. svarbiausios kompiuterinės įrangos gedimai registruojami elektroniniame žurnale. Už gedimų registravimą atsakingas Informacinės sistemos administratorius.

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės turi atitikti šiuos reikalavimus:

6.1. Informacinės sistemos tarnybinėse stotyse ir Informacinės sistemos naudotojų kompiuteriuose turi būti naudojama tik legali, Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

6.2. operatyviai įdiegiami Informacinės sistemos tarnybinių stočių ir pagrindinio Informacinės sistemos tvarkytojo kompiuterizuotų darbo vietų kompiuterinės įrangos, operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

6.3. programinės įrangos diegimą, gedimų šalinimą ir konfigūravimą turi teisę atlikti tik Informacinės sistemos administratorius arba kitas įgaliotas asmuo;

6.4. Informacinės sistemos tarnybinėse stotyse turi būti įrašomi ir saugomi duomenys apie Informacinės sistemos tarnybinių stočių ir taikomosios programinės įrangos įjungimą, išjungimą, informacinės sistemos parametrų pakeitimus, sėkmingus ir nesėkmingus bandymus registruotis Informacinės sistemos tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje, visus informacinės sistemos naudotojų vykdomus veiksmus, naudotojų teisių ir naudotojų grupių pakeitimus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant naudotojo identifikatorių, įvykio datą ir tikslų laiką, įvykio rūšį, įvykio rezultatą. Šie duomenys turi būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę;

6.5. Informacinės sistemos audituojami veiksmai turi būti saugomi ne trumpiau kaip 30 dienų; draudžiama trinti, keisti audituojamus veiksmus, kol nesibaigęs audito duomenų saugojimo terminas;

6.6. fiksuojami Informacinės sistemos naudotojų, kuriems suteikta teisė tvarkyti Informacinės sistemos duomenis, veiksmai;

6.7. programinei įrangai testuoti turi būti naudojama atskira testavimo aplinka;

6.8. Informacinės sistemos tinkle turi būti įdiegtos automatinės įsilaužimo aptikimo sistemos;

6.9. pagrindinėse Informacinės sistemos tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

6.10. draudžiama slaptažodžius saugoti programiniame kode.

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės turi atitikti šiuos reikalavimus:

7.1. Informacinės sistemos tarnybinės stotys, Informacinės sistemos pagrindinio tvarkytojo naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, turi būti atskirta nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami, ugniasienės sukonfigūruotos taip, kad blokuotų visą įeinantį ir išeinantį, išskyrus su informacinės sistemos funkcionalumu ir administravimu susijusį, duomenų srautą;

7.2. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrinamas naudojant šifravimą, virtualų privatų tinklą (VPN) (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones;

7.3. Informacinės sistemos programinė įranga turi būti apsaugota 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*);

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

7.5. naudotojų nuotoliniam prisijungimui prie Informacinės sistemos turi būti naudojamas HTTPS protokolas;

7.6. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę. Ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

7.7. interneto svetainėje, pasiekiamoje iš viešųjų elektroninių ryšių tinklų, šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų; sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų;

7.8. interneto svetainėje, pasiekiamoje iš viešųjų elektroninių ryšių tinklų, turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė;

7.9. interneto svetainėje, pasiekiamoje iš viešųjų elektroninių ryšių tinklų, svetainės naudotojams neturi būti rodomi klaidų pranešimai apie svetainės programinį kodą ar tarnybinę stotį;

7.10. tarnybinėje stotyje, kurioje yra svetainė, pasiekiama iš viešųjų elektroninių ryšių tinklų, turi būti leidžiama naudoti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus;

7.11. interneto svetainėje, pasiekiamoje iš viešųjų elektroninių ryšių tinklų, turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*).

8. Patalpų ir aplinkos saugumo užtikrinimo priemonės turi atitikti šiuos reikalavimus:

8.1. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės;

8.2. Informacinės sistemos tarnybinių stočių patalpoje įrengti gaisro ir judesio davikliai turi būti prijungti prie pastato vietinės signalizacijos pulto;

8.3. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų, asmenys, nesusiję su Informacinės sistemos tvarkymu, patekti į šias patalpas gali tik lydimi Informacinės sistemos administratoriaus;

8.4. turi veikti patekimo į patalpas kontrolės sistema;

8.5. patalpose turi būti naudojami nepertraukiamo elektros maitinimo šaltiniai;

8.6. patekimas į Informacinės sistemos tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės kopijos, turi būti kontroliuojamas šiose taisyklėse nustatyta tvarka.

9. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

9.1. Informacinės sistemos duomenų bazės veiksmų žurnale fiksuojami elektroninės informacijos pakeitimą atlikusio Informacinės sistemos naudotojo duomenys ir pakeitimo laikas;

9.2. kiekvienas naudotojas ar informacinės sistemos administratorius, prieš naudodamasis Informacine sistema, turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone;

9.3. kiekvienam naudotojui Informacinėje sistemoje suteikiamos tik tiesioginėms pareigoms vykdyti būtinos teisės;

9.4. baigus darbą ar pasitraukiant iš darbo vietos Informacinėje sistemoje turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo Informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai ar jų kopijos darbo vietoje padedami į pašaliniams asmenims neprieinamą vietą;

9.5. Informacinės sistemos naudotojui neatliekant jokių veiksmų Informacinėje sistemoje 15 minučių, Informacinės sistemos taikomoji programinė įranga automatiškai užsirakina ir naudotis Informacine sistema galima tik pakartotinai patvirtinus savo tapatybę;

9.6. Informacinės sistemos naudotojų darbo vietose naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (USB, CD/DVD ir kt.);

9.7. atitikties vertinimas atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

9.8. per metus ne mažiau kaip 90 proc. laiko visą parą užtikrinamas Informacinės sistemos prieinamumas.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

10. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

10.1. Informacinės sistemos duomenis įrašyti, keisti, atnaujinti ir naikinti turi teisę tik Informacinės sistemos naudotojai pagal nustatytas prieigos teises;

10.2. administravimo posistemyje tvarkomus duomenis įvesti, keisti, atnaujinti ar naikinti turi teisę tik Informacinės sistemos administratorius;

10.3. Informacinės sistemos duomenys įvedami, atnaujinami, keičiami ir naikinami Informacinės sistemos nuostatuose nustatyta tvarka;

10.4. duomenų įvedimas, pakeitimas, atnaujinimas ir naikinimas registruojami Informacinės sistemos duomenų bazės veiksmų žurnale, nurodant Informacinės sistemos naudotoją, prisijungimo datą, laiką ir atliktus veiksmus. Šie įrašai prieinami tik Informacinės sistemos administratoriui ir saugomi ne trumpiau kaip 1 metus.

11. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

11.1. Informacinės sistemos duomenų kopijos automatiniu būdu, esant aktyviai Informacinės sistemos duomenų bazei, daromos kiekvieną darbo dieną. Atsarginės Informacinės sistemos duomenų kopijos saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota;

11.2. prarasti, iškraipyti ar sunaikinti Informacinės sistemos duomenys turi būti atkuriami iš Informacinės sistemos duomenų atsarginių kopijų. Už Informacinės sistemos duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas paslaugų teikėjas, su kuriuo sudaryta virtualių serverių nuomos sutartis. Nutraukus virtualių serverių nuomos sutartį, už Informacinės sistemos duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas Informacinės sistemos administratorius;

11.3. informacija apie elektroninės informacijos kopijavimą (kopijos įrašymo data ir laikas) automatiškai fiksuojama ir saugoma Informacinės sistemos tarnybinės stoties veiksmų žurnale.

12. Saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų tvarka:

12.1. duomenys iš susijusių registrų ir informacinių sistemų gaunami ir jiems teikiami šių registrų ir informacinių sistemų valdytojų ir Informacinės sistemos tvarkytojo sudarytose duomenų teikimo ir gavimo sutartyse numatyta tvarka;

12.2. Informacinės sistemos duomenys kitai informacinei sistemai perduodami laikantis Informacinės sistemos nuostatuose, Informacinės sistemos saugos politiką įgyvendinančiuose dokumentuose nurodytų reikalavimų;

12.3. duomenų teikėjai duomenis Informacinei sistemai teikia Informacinės sistemos nuostatų nustatyta tvarka;

12.4. už duomenų, gaunamų iš susijusių registrų ir kitų informacinių sistemų, atnaujinimo procesą Informacinėje sistemoje yra atsakingas Informacinės sistemos administratorius.

13. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

13.1. Informacinės sistemos naudotojai, pastebėję duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informacinės sistemos administratoriui;

13.2. Informacinės sistemos administratorius apie saugos pažeidimus informuoja saugos įgaliotinį, imasi visų įmanomų veiksmų neteisėtai veiklai užkirsti bei išnagrinėja Informacinės sistemos duomenų bazės veiksmų žurnalo įrašus, siekdamas nustatyti neteisėtos veiklos šaltinį, laiką ir veiksmus;

13.3. saugos įgaliotinis, gavęs pranešimą apie vykdomą neteisėtą veiklą, inicijuoja elektroninės informacijos saugos incidento valdymo veiksmus, kurie aprašyti Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plane.

14. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo (toliau – pokyčiai) tvarka:

14.1. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami Informacinės sistemos tvarkytojo ir (ar) Informacinės sistemos valdytojo iniciatyva, sprendimą priima Informacinės sistemos valdytojas;

14.2. pokyčių projektavimą ir kūrimą atlieka Informacinės sistemos pagrindinio tvarkytojo paskirti atsakingi darbuotojai arba įstatymų nustatyta tvarka pasirinkti paslaugų tiekėjai tam skirtoje kūrimo aplinkoje. Atsakomybė už pokyčių įgyvendinimo sprendimus nustatoma pokyčių projektavimo ir kūrimo dokumentacijoje;

14.3. prieš atliekant keitimus, kurių metu gali iškilti grėsmė Informacinės sistemos elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pakeitimai turi būti išbandomi testavimo aplinkoje;

14.4. įgyvendinant pokyčius, kurių metu galimi Informacinės sistemos veikimo sutrikimai, Informacinės sistemos administratorius privalo ne vėliau kaip prieš vieną darbo dieną iki planuojamų pokyčių vykdymo pradžios informuoti (elektroniniu paštu, faksu ar kitomis priemonėmis) Informacinės sistemos naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

14.5. atlikęs pokyčių testavimą arba, jei testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, Informacinės sistemos administratorius gali pradėti įgyvendinti pokyčius;

14.6. jeigu testavimas sėkmingas, pokyčiai perkeliami į gamybinę aplinką;

14.7. visi pokyčiai registruojami ir prireikus apie tai informuojami Informacinės sistemos naudotojai;

14.8. Informacinės sistemos administratorius Informacinės sistemos naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi Informacine sistema pakitimus, kurie yra susiję su jų atliekamomis funkcijomis ir kurių atsiradimas susijęs su įvykdytais arba vykdomais pokyčiais;

14.9. Informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINEI SISTEMAI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

15. Reikalavimai Informacinei sistemai funkcionuoti reikalingoms paslaugoms (projektavimo, aptarnavimo ir priežiūros) ir jų teikėjams nustatomi šių paslaugų teikimo sutartyse.

16. Paslaugos teikėjas, teikiantis virtualių serverių nuomos paslaugą, atsakingas už Informacinės sistemos kompiuterinės įrangos saugos priemonių įgyvendinimą, tarnybinių stočių patalpų ir aplinkos saugumą, rezervinių duomenų kopijų darymą ir duomenų atkūrimą jų praradimo atveju.

17. Informacinės sistemos administratorius suteikia prieigos prie Informacinės sistemos duomenų teisę (peržiūrėti Informacinės sistemos duomenis, atlikti užklausas Informacinėje sistemoje, vykdyti veiksmus su Informacinės sistemos duomenimis ir kt.), fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotiems asmenims paslaugų teikimo sutartyje nurodytam laikotarpiui jų nustatytoms funkcijoms atlikti.

18. Perkant paslaugas, darbus ar įrangą, susijusią su informacine sistema, pirkimo dokumentuose turi būti iš anksto nustatyta, kad paslaugos teikėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams, nustatytiems 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“.

19. Prieš suteikiant trečiosioms šalims loginę arba fizinę prieigą prie Informacinės sistemos resursų, saugos įgaliotinis organizuoja trečiųjų šalių atstovų informavimą apie taikytinus informacijos saugumo reikalavimus ir atsakomybę.

20. Pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui, Informacinės sistemos administratorius panaikina paslaugų teikėjo įgaliotų asmenų prieigos prie Informacinės sistemos programinių, techninių ir kitų resursų teisę ir apie tai juos informuoja.

_____

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. spalio 2 d.
įsakymu Nr. V-1065
(Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. lapkričio 26 d.
įsakymo Nr. V-2743 redakcija)

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Veiklos tęstinumo valdymo planas) aprašomos procedūros, kurių būtina laikytis atkuriant Visuomenės sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) veiklą įvykus elektroninės informacijos saugos incidentui ir (ar) kibernetiniam incidentui (toliau - saugos incidentas) ir vykdomas įvykus elektroninės informacijos saugos incidentui, kuris gali sudaryti neteisėto prisijungimo prie Informacinės sistemos galimybę, sutrikdyti ar pakeisti Informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

2. Veiklos tęstinumo valdymo planas parengtas vadovaujantis Saugos dokumentų turinio gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 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“ (toliau – Organizaciniai ir techniniai kibernetinio saugumo reikalavimai), Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas).

3. Veiklos tęstinumo valdymo planas privalomas Informacinės sistemos valdytojui, Informacinės sistemos tvarkytojams, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui bei saugos įgaliotiniui, asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – Kibernetinio saugumo vadovas).

4. Saugos incidento metu patirti nuostoliai Informacinės sistemos veiklai atkurti, įvykus saugos incidentui, finansuojami valstybės biudžeto (Informacinės sistemos valdytojo ir (ar) tvarkytojo), kitų finansavimo šaltinių lėšomis.

5. Informacinės sistemos saugos įgaliotinio, Informacinės sistemos administratoriaus, Informacinės sistemos naudotojų ir Kibernetinio saugumo vadovo įgaliojimai ir veiksmai saugos incidento metu yra nurodyti Visuomenės sveikatos stebėsenos informacinės sistemos veiklos atkūrimo detaliajame plane (1 priedas).

6. Informacinės sistemos veikla laikoma atkurta, kai Informacinės sistemos naudotojai, naudodamiesi Informacine sistema, vėl gali atlikti savo funkcijas.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

7. Veiklos tęstinumo valdymo grupės sudėtis:

7.1. vadovas – Higienos instituto Sveikatos informacijos centro vadovas;

7.2. vadovo pavaduotojas – Higienos instituto Visuomenės sveikatos technologijų centro vadovas;

7.3. nariai:

7.3.1. Higienos instituto Bendrųjų reikalų skyriaus vadovas;

7.3.2. Informacinės sistemos saugos įgaliotinis;

7.3.3. Kibernetinio saugumo vadovas.

8. Užtikrindama Informacinės sistemos veiklos tęstinumą, Veiklos tęstinumo valdymo grupė vykdo šias funkcijas:

8.1. analizuoja elektroninės informacijos saugos incidentus ir priima sprendimus Informacinės sistemos veiklos tęstinumo valdymo klausimais;

8.2. bendrauja su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

8.3. bendrauja su susijusių registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

8.4. bendrauja su teisėsaugos ir kitomis institucijomis, atsakingomis už nacionalinį elektroninių ryšių tinklų ir informacijos saugumą;

8.5. kontroliuoja finansinių ir kitų išteklių, reikalingų Informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, naudojimą;

8.6. organizuoja darbuotojų, Informacinės sistemos techninės įrangos gabenimą;

8.7. vykdo Informacinės sistemos veiklos atkūrimo priežiūrą ir koordinuoja veiklos atkūrimo veiksmus bei kitas pavestas funkcijas.

9. Veiklos atkūrimo grupės sudėtis:

9.1. vadovas – Higienos instituto Sveikatos informacijos centro Registrų skyriaus vadovas;

9.2. vadovo pavaduotojas – Informacinės sistemos administratorius;

9.3. nariai:

9.3.1. Informacinės sistemos saugos įgaliotinis;

9.3.2. Higienos instituto Registrų skyriaus specialistas.

10. Veiklos atkūrimo grupė vykdo šias funkcijas:

10.1. organizuoja Informacinės sistemos tarnybinių stočių veikimo atkūrimą;

10.2. organizuoja Informacinės sistemos tvarkytojo kompiuterių tinklo veikimo atkūrimą;

10.3. organizuoja Informacinės sistemos elektroninės informacijos atkūrimą;

10.4. organizuoja taikomųjų programų tinkamo veikimo atkūrimą;

10.5. organizuoja pagrindinio Informacinės sistemos tvarkytojo darbuotojų kompiuterių veikimo atkūrimą;

10.6. vykdo kitas veiklos atkūrimo grupei pavestas funkcijas, susijusias su Informacinės sistemos veiklos atkūrimu.

11. Veiklos tęstinumo valdymo ir veiklos atkūrimo grupės tarpusavyje komunikuoja tiesiogiai, telefonu arba elektroniniu paštu.

12. Informacinės sistemos veikla atkuriama pagal Informacinės sistemos veiklos atkūrimo detalųjį planą (1 priedas), už kurio parengimą ir aktualizavimą yra atsakingas Informacinės sistemos saugos įgaliotinis.

13. Veiklos tęstinumo valdymo grupė organizuoja susirinkimą įvykus esminiams Informacinės sistemos pokyčiams. Veiklos tęstinumo valdymo grupė, atlikusi situacijos analizę,

susisiekia su Veiklos atkūrimo grupe ir informuoja apie esamą padėtį ir priimtus sprendimus dėl Informacinės sistemos veiklos atkūrimo.

14. Apie įvykdytus veiklos atkūrimo etapus atsakingi asmenys nedelsdami informuoja Veiklos atkūrimo grupės vadovą.

15. Saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka.

16. Elektroninės informacijos saugos incidentai registruojami Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnale (2 priedas), už kurio pildymą atsakingas Informacinės sistemos administratorius.

17. Įvykus saugos incidentui:

17.1. Informacinės sistemos naudotojai privalo nedelsdami žodžiu ar raštu pranešti Informacinės sistemos administratoriui apie įvykusį saugos incidentą. Patys Informacinės sistemos naudotojai neturi teisės imtis jokių veiksmų;

17.2. Informacinės sistemos administratorius, gavęs pranešimą apie saugos incidentą, nedelsdamas turi imtis veiksmų, reikalingų saugos incidentui stabdyti. Apie saugos incidentą Informacinės sistemos administratorius, įvertinęs incidento reikšmingumą, žodžiu ar raštu pagal kompetenciją informuoja Informacinės sistemos saugos įgaliotinį ir Kibernetinio saugumo vadovą. Įvykis aprašomas, nurodant saugos incidento vietą, laiką, pobūdį ir kitą su įvykiu susijusią informaciją;

17.3. vadovaudamasis Nacionaliniu kibernetinių incidentų valdymo planu, Kibernetinio saugumo vadovas nustato prioritetą kibernetinio pobūdžio saugos incidentams valdyti, tirti ir šalinti bei apie juos informuoja Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos Kibernetinių incidentų valdymo ir pranešimo apie kibernetinius incidentus tvarkos aprašo (3 priedas) nustatyta tvarka;

17.4. Informacinės sistemos saugos įgaliotinis apie saugos incidentą žodžiu arba raštu nedelsdamas informuoja Informacinės sistemos vadovą, Veiklos tęstinumo valdymo grupės vadovą ir Veiklos atkūrimo grupės vadovą;

17.5. Informacinės sistemos saugos įgaliotinis įrašo informaciją apie saugos incidentą į elektroninės informacijos saugos incidentų registravimo žurnalą (2 priedas), vadovauja veiklos atkūrimo detaliajame plane nurodytiems veiksmams;

17.6. Informacinės sistemos administratorius atkuria Informacinės sistemos techninės ir programinės įrangos veikimą, kompiuterių tinklo veiklą, Informacinės sistemos elektroninę informaciją, Informacinės sistemos techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir nedelsdamas apie atliktus veiksmus informuoja Informacinės sistemos saugos įgaliotinį, Veiklos valdymo grupės vadovą ir Veiklos atkūrimo grupės vadovą;

17.7. Informacinės sistemos saugos įgaliotinis, Kibernetinio saugumo vadovas kartu su Informacinės sistemos administratoriumi organizuoja žalos Informacinės sistemos elektroninei informacijai, Informacinės sistemos techninei, programinei įrangai vertinimą, koordinuoja Informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą;

17.8. saugos incidentui išplitus už Informacinės sistemos valdytojo ir Informacinės sistemos įstaigos ribų, Informacinės sistemos administratorius nedelsdamas informuoja su saugos incidentu susijusius paslaugų teikėjus ir (ar) kitas institucijas, atsižvelgia į jų rekomendacijas;

17.9. Valdymo grupė, atsižvelgusi į saugos incidento pobūdį, parengia Informacinės sistemos valdytojo vadovui tarnybinį pranešimą apie įvykusį saugos incidentą, atliktus veiksmus ir pasekmes.

18. Elektroninės informacijos saugos incidentai registruojami Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnale (2 priedas), už kurio pildymą atsakingas Informacinės sistemos administratorius.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

19. Parengtų ir Higienos instituto Registrų skyriuje saugomų dokumentų sąrašas:

19.1. Informacinės sistemos techninio aprašymo (specifikacijos) kopija, kurioje nurodyti Informacinės sistemos techninės ir programinės įrangos parametrai. Už Informacinės sistemos techninės ir programinės įrangos priežiūrą atsakingas Informacinės sistemos administratorius, kuriam keliami kvalifikaciniai reikalavimai, nurodyti Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. įsakymu Nr. V-405 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“. Nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, jį pavaduoti gali kitas Higienos instituto direktoriaus paskirtas darbuotojas, kurio kompetencijos lygis informacinių technologijų srityje atitinka Informacinės sistemos administratoriui keliamus reikalavimus;

19.2. Higienos instituto pastato, kuriame yra tarnybinės stotys, patalpų planai, tarnybinių stočių fizinio ir loginio sujungimo schemos;

19.3. Informacinės sistemos elektroninės informacijos teikimo, Informacinės sistemos programinės įrangos priežiūros ir virtualių serverių nuomos sutarčių kopijos;

19.4. Informacinės sistemos techninės ir programinės įrangos sąrašai, kuriuose nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos. Atsarginės laikmenos su programinės įrangos kopijomis turi būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra informacinės sistemos tarnybinės stotys;

19.5. Informacinės sistemos duomenų rezervinių kopijų kūrimo instrukcija, kurioje nurodyta laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

19.6. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu.

20. Veiklos tęstinumo valdymo plano 19 punkte nurodytų dokumentų, susegtų į bylą, kopijas saugo Informacinės sistemos saugos įgaliotinis. Už Informacinės sistemos programinės įrangos priežiūrą atsakingas Informacinės sistemos administratorius.

IV SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

21. Veiklos tęstinumo valdymo plano veiksmingumo išbandymą organizuoja Informacinės sistemos saugos įgaliotinis.

22. Veiklos tęstinumo valdymo plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus.

23. Prieš įdiegiant naujus Informacinės sistemos komponentus, pradedant teikti naujas paslaugas arba pasikeitus Informacinės sistemos veiklos aplinkai, Informacinės sistemos saugos įgaliotinis turi peržiūrėti Veiklos tęstinumo valdymo planą ir, esant reikalui, atlikti neeilinį Veiklos tęstinumo valdymo plano veiksmingumo išbandymą simuliavimo būdu pagal saugos incidento situacijos scenarijų.

24. Išbandžius Veiklos tęstinumo valdymo plano veiksmingumą, Informacinės sistemos saugos įgaliotinis turi parengti Veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitą ir pateikti ją Informacinės sistemos tvarkytojui. Veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitos forma pateikta 4 priede.

25. Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Visuomenės sveikatos stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
1 priedas

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Įvykis, sukeliantis elektroninės informacijos saugos incidentą	**Pasekmės likvidavimo veiksmai**	**Atsakingi vykdytojai**
1. Patalpų pažeidimas arba praradimas, stichinė nelaimė	1.1.1. jeigu būtina, skelbkite pavojų ir informuokite Veiklos tęstinumo valdymo grupės vadovą;	Pavojų pastebėjęs darbuotojas
1.1. Higienos instituto patalpose	1.1.2. praneškite specialiosioms tarnyboms;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.3. iškvieskite Veiklos tęstinumo valdymo grupės narius į saugią vietą;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.4. informuokite Informacinės sistemos Veiklos atkūrimo grupės vadovą;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	1.1.5. iškvieskite Informacinės sistemos Veiklos atkūrimo grupės narius į saugią vietą;	
	1.1.6. vykdykite specialiųjų tarnybų nurodymus;	Visi Higienos instituto darbuotojai
	1.1.7. organizuokite darbuotojų evakuaciją, suskaičiuokite evakuotus darbuotojus;	Veiklos tęstinumo valdymo grupės vadovo pavaduotojas
	1.1.8. informuokite specialiąsias tarnybas apie dingusius darbuotojus;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.9. gavę rekomendacijas iš specialiųjų tarnybų, informuokite	

	darbuotojus, kaip elgtis esant susidariusiai situacijai;	
	1.1.10. esant būtinybei, išjunkite ir užrakinkite visą įrangą;	
	1.1.11. įvertinkite pažeidimus ir padarytus nuostolius;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.12. informuokite darbuotojus apie darbo funkcijų vykdymo aplinkybes;	
	1.1.13. nustatykite, ar buvo prarasta įranga;	Veiklos atkūrimo grupės vadovas
	1.1.14. įrangos praradimo atveju informuokite Veiklos tęstinumo valdymo grupę;	Veiklos atkūrimo grupės vadovas
	1.1.15. vykdykite teisėsaugos institucijų ir (arba) draudimo įmonės nurodymus, pateikdami reikiamus duomenis apie įvykį;	
	1.1.16. prireikus perskirstykite, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų atkurtas Informacinės sistemos veikimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.17. trūkstant išteklių, kreipkitės į Informacinės sistemos valdytoją dėl papildomų resursų skyrimo;	
	1.1.18. įsigijus įrangą, atkurkite Informacinės sistemos darbingumą.	
1.2. Paslaugos teikėjo, kurio patalpose yra Informacinės sistemos programinė įranga, patalpos	1.2.1. nustačius Informacinės sistemos programinės įrangos pažeidimus arba praradimą nedelsiant informuokite Informacinės sistemos tvarkytoją;	Veiklos atkūrimo grupės vadovas
	1.2.2. vadovaudamasis paslaugos teikimo sutartyje nustatytais įsipareigojimais, vykdykite Informacinės sistemos programinės įrangos atkūrimo darbus.	Paslaugos teikėjas
2. Gaisras	2.1.1. pastebėjus gaisro židinį, stenkitės jį užgesinti kuo anksčiau;	Pavojų pastebėjęs darbuotojas
2.1. Higienos instituto patalpos	2.1.2. jeigu būtina, skelbkite pavojų ir praneškite priešgaisrinei gelbėjimo tarnybai;	Pavojų pastebėjęs darbuotojas
	2.1.3. informuokite Veiklos tęstinumo valdymo grupės vadovą;	Pavojų pastebėjęs darbuotojas

	2.1.4. iškvieskite Veiklos tęstinumo valdymo grupę į saugią vietą;	Veiklos tęstinumo valdymo grupės vadovas
	2.1.5. informuokite Veiklos atkūrimo grupės vadovą; 2.1.6. iškvieskite Veiklos atkūrimo grupę;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas
	2.1.7. vykdykite specialiųjų tarnybų nurodymus;	Visi darbuotojai
	2.1.8. jeigu būtina, organizuokite darbuotojų evakuaciją, suskaičiuokite evakuotus darbuotojus;	Veiklos tęstinumo valdymo grupės vadovas
	2.1.9. informuokite specialiąsias tarnybas apie dingusius darbuotojus; 2.1.10. gavę rekomendacijas iš specialiųjų tarnybų, informuokite darbuotojus, kaip elgtis pavojaus zonoje;	Veiklos tęstinumo valdymo grupės vadovas
	2.1.11. likvidavus gaisrą įvertinkite pažeidimus ir patirtus nuostolius;	
	2.1.12. esant poreikiui perskirstykite, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų atkurtas Informacinės sistemos veikimas;	Veiklos atkūrimo grupės vadovas
	2.1.13. nesant pakankamo rezervo, kreipkitės į Informacinės sistemos valdytoją dėl papildomų resursų skyrimo;	Veiklos atkūrimo grupės vadovas
	2.1.14. įsigijus įrangą, atkurkite Informacinės sistemos darbingumą.	
2.2. Paslaugos teikėjo, kurio patalpose yra Informacinės sistemos programinė įranga, patalpos	2.2.1. Nustačius Informacinės sistemos programinės įrangos pažeidimus arba praradimą, nedelsdamas informuokite Informacinės sistemos tvarkytoją;	Paslaugos teikėjas
	2.2.2. vadovaudamiesi paslaugos teikimo sutartyje nustatytais įsipareigojimais, vykdykite Informacinės sistemos programinės įrangos atkūrimo darbus.	
3. Pagrindinės kompiuterinės įrangos	3.1. Nustačius Informacinės sistemos programinės įrangos pažeidimus arba praradimą nedelsdami informuokite Informacinės	Paslaugos teikėjas

praradimas, nepakenkiant patalpų funkcionalumui	sistemos tvarkytoją;	
	3.2. vadovaudamiesi paslaugos teikimo sutartyje nustatytais įsipareigojimais, vykdykite Informacinės sistemos programinės įrangos atkūrimo darbus.	Veiklos tęstinumo valdymo grupės vadovas
4. Pagrindinių duomenų praradimas pažeidus ar kitaip sugadinus centrinę duomenų saugyklą	4.1. nutraukite paslaugų teikimą Informacinės sistemos naudotojams, jeigu tai kelia pavojų prarasti duomenis ir kitaip pažeisti Informacinės sistemos funkcionalumą;	Veiklos atkūrimo grupės vadovas
	4.2. informuokite Informacinės sistemos naudotojus, jeigu tai sukelia veiklos sutrikimus;	
	4.3. jeigu Informacinės sistemos duomenys prarasti ar jie tapo prieinami leidimo neturintiems asmenims, praneškite teisėsaugos organams;	
	4.4. vykdykite teisėsaugos organų nurodymus, pateikdami reikiamą informaciją apie įvykį;	
	4.5. atkurkite Informacinės sistemos veikimą;	
	4.6. nustatykite, ar atkurti duomenys yra patikimi;	Veiklos atkūrimo grupės vadovas
	4.7. jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinkite jas;	Veiklos atkūrimo grupės vadovas
	4.8. atkurkite Informacinės sistemos duomenis iš paskutinės geros atsarginės kopijos;	
	4.9. visiškai atkurkite Informacinės sistemos veiklą ir visas Informacinės sistemos naudotojų galimybes naudotis Informacine sistema.	
5. Informacinės sistemos veiklos sutrikdymas dėl kibernetinės saugos	5.1. nutraukite paslaugų teikimą Informacinės sistemos naudotojams ir informuokite juos apie veiklos sutrikimus;	Veiklos atkūrimo grupės vadovas
	5.2. nustatykite trikdžių šaltinį;	Kibernetinio saugumo vadovas
	5.3. praneškite nacionaliniam kibernetinio saugumo centrui, esant	

incidentų	nusikalstamos veiklos požymių praneškite policijai, jei kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais praneškite Valstybinei duomenų apsaugos inspekcijai (nustatytą incidento reikšmės lygį ir kitus duomenis);	
	5.4. patikrinkite, ar neprarasti arba nesugadinti Informacinės sistemos duomenys;	
	5.5. pašalinę trikdžius, atkurkite Informacinės sistemos darbingumą; jeigu būtina, atkurkite duomenis iš rezervinių kopijų.	Veiklos atkūrimo grupės vadovas
6. Elektros ir telekomunikacinių ryšių tiekimo sutrikimai	6.1. Jeigu yra galimybė, nustatykite elektros ir ryšių paslaugų teikimo sutrikimo priežastis;	Veiklos tęstinumo valdymo grupės vadovas
	6.2. kreipkitės į paslaugų teikėją dėl sutrikimų pašalinimo;	
	6.3. informuokite darbuotojus ir pateikite rekomendacijas, kaip elgtis esant susidariusiai situacijai;	
	6.4. pašalinus sutrikimą, atnaujinkite Informacinės sistemos veikimą.	
7. Vandentiekio ar šildymo sistemos avarija	7.1. kreipkitės į specialiąsias tarnybas dėl sutrikimų pašalinimo;	Veiklos tęstinumo valdymo grupės vadovas
	7.2. informuokite darbuotojus ir pateikite rekomendacijas, kaip elgtis esant susidariusiai situacijai;	
	7.3. pašalinus sutrikimą, atnaujinkite Informacinės sistemos veikimą.	Veiklos atkūrimo grupės vadovas

_____

Visuomenės sveikatos stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
2 priedas

(Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20__m. _____ d.

Eil. Nr.	Elektroninės informacijos saugos incidentas					
	Informacinės sistemos tvarkytojo pavadinimas	Požymio kodas	Elektroninės informacijos saugos incidento aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Saugos incidentą pašalino (vardas, pavardė)
1.						
2.						
3.						
4.						

Elektroninės informacijos saugos incidento požymiai:

1 – gaisras; 2 – elektros energijos tiekimo sutrikimai; 3 – įsilaužimo kibernetinis incidentas; 4 – vandentiekio ir šildymo sistemos sutrikimai; 5 – kondicionavimo sistemos sutrikimas; 6 – ryšio sutrikimai; 7 – tarnybinių stočių vagystė arba sugadinimas; 8 – programinės įrangos sugadinimas, praradimas; 9 – vagystė iš duomenų bazės ar jos fizinis sunaikinimas; 10 – kompiuterių ir juose saugomų duomenų praradimas; 11 – pavojingas (įtartinas) radinys; 12 – informacinių išteklių (toliau – RIS) trikdymas, kibernetinis incidentas; 13 – dokumentų praradimas; 14 – duomenų iš duomenų teikėjų negavimas; 15 – dalinis Informacinės sistemos sutrikimas dėl neaiškių priežasčių; 16 – gamtos reiškiniai; 17 – kenkimo programinės įrangos kibernetinis incidentas; 18 – RIS perimetro žvalgybos kibernetinis incidentas; 19 – neteisėta veikla (vagystė, apgavystė ir panašūs kriminalinio pobūdžio kibernetiniai incidentai); 20 – Vientisumo pažeidimo kibernetinis incidentas.

_____

Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano
3 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO IR PRANEŠIMO APIE KIBERNETINIUS INCIDENTUS TVARKOS APRAŠAS

1. Įvykus kibernetinės saugos incidentui, Nacionaliniam kibernetinio saugumo centrui (toliau priede – Centras) pranešama apie:

1.1. didelio poveikio kibernetinį incidentą – ne vėliau kaip per vieną valandą nuo jo nustatymo;

1.2. vidutinio poveikio kibernetinį incidentą – ne vėliau kaip per 4 valandas nuo jo nustatymo;

1.3. nereikšmingo poveikio kibernetinį incidentą – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

2. Pranešime apie didelio ir vidutinio poveikio kibernetinį incidentą turi būti nurodyta:

2.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

2.2. trumpas kibernetinio incidento apibūdinimas;

2.3. tikslus laikas, kada kibernetinis incidentas įvyko ir kada buvo nustatytas;

2.4. kibernetinio incidento kategorija;

2.5. kibernetinio incidento šalinimo tvarka (turi būti nurodyta, ar tai prioritetas, ar ne);

2.6. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita;

2.7. pranešime apie nereikšmingą kibernetinį incidentą turi būti pateikta apibendrinta informacija apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo pateikimo dienos, skaičių.

3. Centrui turi būti pateikiama kibernetinio incidento tyrimo ataskaita:

3.1. didelio poveikio kibernetinio incidento valdymo būklę – ne vėliau kaip per 4 valandas nuo jo nustatymo ir ne rečiau kaip kas 4 valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

3.2. vidutinio poveikio kibernetinio incidento valdymo būklę – ne vėliau kaip per 24 valandas nuo jo nustatymo ir ne rečiau kaip kas 24 valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

3.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per 4 valandas nuo jų suvaldymo ar pasibaigimo.

4. Didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitoje turi būti nurodyta žinoma informacija:

4.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

4.2. informacinės infrastruktūros ir informacinių išteklių (toliau – RIS), kuriuose nustatytas kibernetinis incidentas, tipas (informacinė sistema, elektroninių ryšių tinklas, tarnybinė stotis ir panašiai);

4.3. kibernetinio incidento veikimo trukmė;

4.4. kibernetinio incidento šaltinis;

4.5. kibernetinio incidento požymiai;

4.6. kibernetinio incidento veikimo metodas;

4.7. galimos kibernetinio incidento pasekmės;

4.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

4.9. kibernetinio incidento būsena (aktyvus, pasyvus);

4.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

4.11. galimos kibernetinio incidento valdymo priemonės.

4.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Nacionalinio kibernetinių incidentų valdymo plano 23 punktu.

5. Įvertinus, kad negalima savarankiškai ištirti ar suvaldyti kibernetinio incidento, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo, kreipiamasi pagalbos į Centrą.

6. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ir atkuriama įprasta informacinės sistemos veikla, atitinkanti Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2018 m. balandžio 10 d. įsakymu Nr. V-405 „Dėl Visuomenės sveikatos stebėsenos informacinės sistemos nuostatų ir Visuomenės sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“, nustatytus reikalavimus.

7. Gavus iš Centro, Valstybinės duomenų apsaugos inspekcijos, Lietuvos policijos (toliau kartu – KIVT institucijos), kitų juridinių asmenų ar kitų valstybių arba tarptautinių organizacijų ar institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, informaciją apie galimą kibernetinį incidentą informacinėje sistemoje, imamasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti. Nenustačius kibernetinio incidento požymių, ne vėliau kaip per 4 valandas nuo pranešimo apie kibernetinį incidentą gavimo informuojamos KIVT institucijos.

8. Apie kibernetinius incidentus ir valdymą Centras turi būti informuojamas per Kibernetinio saugumo informacinį tinklą, o nesant galimybės – kitomis saugiomis informacijos perdavimo priemonėmis.

9. Po kibernetinio incidento suvaldymo ar pasibaigimo atliekama jo analizė. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

10. Ištyrus Registre įvykusį kibernetinį incidentą, išanalizuojama, įvertinama informacija, susijusi su kibernetiniu incidentu, ir imamasi priemonių:

10.1. ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikiami kibernetinio incidento analizės rezultatai Centrui ir kibernetinio saugumo informaciniame tinkle paskelbiama susisteminta ir aktuali neįslaptinta informacija apie kibernetinio incidento nustatymą ir suvaldymą;

10.2. imamasi priemonių, kad būtų pašalintas ryšių ir informacinės sistemos pažeidžiamumas;

10.3. įvertinama ryšių ir informacinės sistemos rizika ir atitiktis Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

10.4. nustačius teisinio reglamentavimo spragų, pakeičiami savo kibernetinio saugumo teisės aktai ir (ar) inicijuojami kitų institucijų priimtų teisės aktų pakeitimai.

11. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami konkrečiai kategorijai nustatyti žemiau pateiktoje lentelėje:

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsiparegojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
1.	Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*)	1.1. Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ryšių ir informacinės sistemos (toliau – RIS) veiklą ir (ar) teikiamas paslaugas	N				V					D					P		
		1.2. Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas	N																
2.	Kenkimo programinė įranga (angl. *malicious software / code*) Programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti	2.1. Aptikta moderni kenkimo programinė įranga (angl. *advanced persistent threat, APT*)					V					D					P		
		2.2. RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys“ (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsiparegojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą					V					D					P			
		2.4. Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja	N				V													
		2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus	N				V					D					P			
3.	Informacijos rinkimas (angl. *information*	3.1. RIS paketų / informacijos perėmimas					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsiparegojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	gathering) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus	3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)					V					D					P			
		3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N				V													
		3.4. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją	N				V													
4.	Mėginimas įsilaužti (angl.	4.1. Išnaudojamas vienas ar keli					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsiparegojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	intrusion attempts) Mėginimas įsilaužti arba sutrikdyti RIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*)	nežinomi (angl. *zero day*) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią RIS																		
		4.2. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai	N				V					D					P			
		4.3. Vidinė RIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita)					V					D					P			
		4.4. Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisijungti prie RIS parenkant slaptažodžius	N				V													
5.	Įsilaužimas (angl. *intrusions*) Sėkmingas įsilaužimas ir (ar) neteisėtas RIS,	5.1. Veiksmai prieš RIS ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, RIS ar jos dalies pažeidimas, sutrikdantis					V					D					P			

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsiparegojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*)	RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS naudotojų pasitikėjimą jais																	
		5.2. Gaunama neteisėta prieiga prie RIS, taikomosios programinės įrangos ar paslaugos					V					D					P		
6.	Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*) Veiksmai, kuriais trikdoma RIS veikla, teikiamos paslaugos (angl. *DoS, DDoS*), RIS ar jos dalies pažeidimas, sutrikdantis RIS ir (ar) jos teikiamas	6.1. Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas					V					D					P		
		6.2. Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui	N				V												

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	paslaugas (angl. *sabotage, outage*)	6.3. Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui	N				V												
7.	Informacijos turinio saugumo pažeidimai (angl. *information content security*) Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas (angl. *unauthorised access to information, unauthorised modification of information*)	7.1. Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai ir (ar) teikiamoms paslaugoms					V					D					P		
		7.2. Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas	N				V					D					P		
8.	Neteisėta veikla, sukčiavimas (angl. *fraud*) Vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of*	8.1. Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms	N				V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 %	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	resources), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai																		
9.	Kita Incidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų		N				V					D					P		

Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano
4 priedas

(Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano išbandymo ataskaitos pavyzdys)

VISUOMENĖS SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO ATASKAITA

(Grupės susitikimo data)

Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano išbandyme dalyvavo:

1. _____
2. _____
3. _____

Elektroninės informacijos saugos incidento scenarijus:

Elektroninės informacijos saugos incidento valdymo eiga:

Rasti veiklos tęstinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti Visuomenės sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo planą:

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

_____