LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2015 M. RUGSĖJO 28 D. ĮSAKYMO NR. V-1082 „DĖL VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ, VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ IR VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO“ PAKEITIMO

2020 m. birželio 8 d. Nr. V-1399

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. rugsėjo 28 d. įsakymą Nr. V-1082 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos naudotojų administravimo taisyklių, Vaikų sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių ir Vaikų 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 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“:“.

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

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

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

Sveikatos apsaugos ministras Aurelijus Veryga

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2020 m. gegužės 19 d. raštu Nr. (4.1E)6K-314

Sveikatos apsaugos viceministras
Algirdas Šešelgis
2020-06-05

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Rasa Sinkevičiūtė
2020-06-05

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-28

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vedėja
Vilma Telyčėnienė
2020-05-27

Teisės skyriaus vedėja
Martyna Mickė
2020-06-05

Parengė
R. Jankauskas
2020-05-22

Teisės skyriaus vyriausiasis specialistas
Natanantas Satkus
2020-06-04

Higienos instituto direktorius
Remigijus Jankauskas
2020-05-22

LR sveikatos apsaugos ministerijos Visuomenės sveikatos departamento direktorius
[illegible] Ščeponavičius
2020-05-26

Sveikatos saugos skyriaus vedėja
Dr. Rita Sketerskienė
2020-05-28

9160

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2015 m. rugsėjo 28 d.
įsakymu Nr. V-1082
(Lietuvos Respublikos sveikatos apsaugos
ministro 2020 m. birželio 8 d.
įsakymo Nr. V-1399
redakcija)

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

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

2. Taisyklės parengtos vadovaujantis 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), 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“, ir 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“.

3. Prieigos prie Informacinės sistemos elektroninės informacijos suteikimo principai:

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

3.2. „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

4. Prieš tapdamas Informacinės sistemos naudotoju darbuotojas privalo susipažinti su Reglamentu (ES) 2016/679, Informacinės sistemos duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos duomenų saugos nuostatai), ir saugos politiką

2020 -05- 22

įgyvendinančiais dokumentais (toliau visi kartu – saugos dokumentai) ir pasirašyti Taisyklių priede nustatytos formos pasižadėjimą saugoti Informacinėje sistemoje tvarkomų asmens duomenų paslaptį (priedas), ir turi būti informuotas, kad už saugos reikalavimų nesilaikymą pagal Lietuvos Respublikos įstatymus kyla drausminė, tarnybinė, civilinė, administracinė arba baudžiamoji atsakomybė. Kiekvienas tvarkytojas kaupia ir 3 metus saugo savo įstaigos Informacinės sistemos naudotojų pasižadėjimus saugoti Informacinėje sistemoje tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų.

5. Informacinės sistemos naudotojai:

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

5.2. 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;

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

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

5.5. 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;

5.6. 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, įjungti ekrano užsklandą su slaptažodžiu;

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

6. Informacinės sistemos naudotojams negali būti suteikiamos Informacinės sistemos administratoriaus teisės.

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

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

7.2. 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.);

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

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

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

7.6. diegti tarnybinių stočių programinės įrangos atnaujinimus;

7.7. administruoti Informacinės sistemos tarnybines stotis ir Informacinės sistemos naudotojų kompiuterizuotas darbo vietas;

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

2020 -05- 22

7.9. vykdyti kitas Informacinės sistemos administratoriaus ir naudotojų teises ir pareigas, nurodytas Informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo".

8. 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 ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

9. Informacinės sistemos naudotojų registravimo ir išregistravimo tvarka:

9.1. Informacinės sistemos administratorius, gavęs asmens, turinčio teisinį pagrindą tvarkyti Informacinės sistemos duomenis, prašymą, kuriame nurodyti Informacinės sistemos naudotojo duomenys: vardas, pavardė, pareigos, elektroninio pašto adresas, telefono numeris, įregistruoja ir išregistruoja Informacinės sistemos pagrindinio tvarkytojo ir (ar) kito Informacinės sistemos tvarkytojo (savivaldybės visuomenės sveikatos biuro) naudotojus, taip pat išregistruoja kito Informacinės sistemos tvarkytojo (savivaldybės visuomenės sveikatos biuro) naudotojus, kurie tiesiogiai tvarko vaikų sveikatos duomenis;

9.2. Informacinės sistemos tvarkytojo (savivaldybės visuomenės sveikatos biuro) atsakingas asmuo, gavęs asmens, turinčio teisinį pagrindą tvarkyti Informacinės sistemos vaikų sveikatos duomenis, prašymą, kuriame nurodyti Informacinės sistemos naudotojo duomenys: vardas, pavardė, pareigos, elektroninio pašto adresas, telefono numeris, įregistruoja Informacinės sistemos tvarkytojo (savivaldybės visuomenės sveikatos biuro) naudotojus, kurie tiesiogiai tvarko vaikų sveikatos duomenis;

9.3. gavęs suteiktą vardą ir slaptažodį ir pirmą kartą prisijungęs prie Informacinės sistemos duomenų bazės, Informacinės sistemos naudotojas nedelsdamas pirminį slaptažodį pakeičia nauju ir jį įsimena;

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

9.5. Informacinės sistemos naudotojų duomenys registruojami ir kaupiami Informacinės sistemos duomenų bazėje ir elektroniniame naudotojų registracijos žurnale, kurį pildo Informacinės sistemos administratorius.

10. Slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai:

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

10.2. slaptažodžiui sudaryti neturi būti naudojama asmeninio pobūdžio (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai) informacija;

10.3. programinės įrangos vartotojo autentifikavimo dalys turi drausti automatiškai išsaugoti slaptažodžius;

10.4. nustatytas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius (5 kartai). Neteisingai įvedus slaptažodį didžiausią leistiną skaičių, Informacinė sistema turi užsirakinti ir neleisti informacinės sistemos naudotojui identifikuotis 15 minučių;

10.5. slaptažodis turi būti keičiamas kas 90 dienų. Informacinės sistemos naudotojo teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;

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

2020 -05- 22

10.7. Informacinės sistemos naudotojui pamiršus slaptažodį, jis turi kreiptis į Informacinės sistemos administratorių arba į Informacinės sistemos tvarkytojo vadovo paskirtą atsakingą asmenį;

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

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

10.10. papildomi reikalavimai Informacinės sistemos administratoriaus slaptažodžiams:

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

10.10.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

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

10.11. papildomi reikalavimai Informacinės sistemos naudotojų slaptažodžiams:

10.11.1. slaptažodis turi būti keičiamas ne rečiau kaip kas tris mėnesius;

10.11.2. keičiant slaptažodį, neleidžiama sudaryti slaptažodžio iš buvusių šešių paskutinių slaptažodžių;

10.12. draudžiama slaptažodžius atskleisti kitiems asmenims.

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

11.1. pasibaigus darbo santykiams, Informacinės sistemos naudotojo teisė naudotis Informacine sistema panaikinama;

11.2. teisė dirbti su Informacinės sistemos duomenimis sustabdoma, kai Informacinės sistemos naudotojas nesinaudoja informacine sistema ilgiau kaip 3 mėnesius, kai įstatymų nustatytais atvejais vidinis informacinės sistemos naudotojas nušalinamas nuo darbo (pareigų); pasibaigus tarnybos (darbo) santykiams, vidinio informacinės sistemos naudotojo teisė naudotis informacine sistema panaikinama nedelsiant;

11.3. keičiantis darbuotojo pareiginėms funkcijoms turi būti peržiūrimos jo prieigos prie Informacinės sistemos duomenų teisės;

11.4. apie Informacinės sistemos naudotojo prieigos teisių dirbti su Informacinės sistemos duomenimis panaikinimą ar laikiną sustabdymą Informacinės sistemos tvarkytojo paskirtas atsakingas asmuo elektroniniu laišku informuoja Informacinės sistemos administratorių iš anksto pranešdamas naudotojo prieigos panaikinimo datą ir laiką.

12. Informacinėje sistemoje vykdoma Informacinės sistemos naudotojų paskyrų kontrolė:

12.1. kai Informacinės sistemos naudotojas nesinaudoja Informacine sistema ilgiau nei 3 mėnesius, jo paskyros galiojimas sustabdomas;

12.2. 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.

13. Informacinėje sistemoje vykdoma Informacinės sistemos administratoriaus paskyrų kontrolė:

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

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

14. Draudžiama Informacinės sistemos techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus.

15. 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

2020-05-27

užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais Informacinės sistemos administratorius nušalinamas nuo darbo (pareigų).

16. Nuotolinis Informacinės sistemos naudotojų prisijungimas prie Informacinės sistemos duomenų bazės leistinas per internetinę naudotojo sąsają, naudojant saugius duomenų perdavimo protokolus.

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vedėja
2020 05 27
Vilma Telyčėnienė

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Rasa Sinkevičiūtė
2020-06-05

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-28

2020-05-22
Higienos instituto direktorius
Remigijus Jankauskas

Teisės skyriaus vyriausiasis specialistas
Narimantas Satkus
2020-06-04

Sveikatos saugos skyriaus vedėja
Dr. Rita Skėterskienė
2020-05-26

Vaikų sveikatos stebėsenos informacinės sistemos naudotojų administravimo taisyklių priedas

(Pasižadėjimo saugoti Vaikų sveikatos stebėsenos informacinėje sistemoje tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų forma)

PASIŽADĖJIMAS SAUGOTI VAIKŲ 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 Lietuvos Respublikos ir Europos Sąjungos teisės aktus.

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

2.1. asmens duomenys, suprantami, kaip apibrėžti 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (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);

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 sudaryta 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.

2020 -05- 22

4. Aš įsipareigoju:

4.1. saugoti konfidencialią informaciją;

4.2. tvarkyti konfidencialią informaciją vadovaudamasis 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;

4.4. laikytis Vaikų sveikatos stebėsenos informacinės sistemos duomenų, tame tarpe ir asmens duomenų, saugą reglamentuojančių teisės aktų reikalavimų;

4.5. 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;

4.6. 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)

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-27

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Rasa Sinkevičiūtė
2020-06-05

Elektroninės sveikat... ir informacinių išteklių...
Vilma Telyčė...

Teisės skyriaus vyriausiasis specialist...
Nat...imantas Sa...
2020-06-04

Sveikatos saugos skyriaus vedėja
Dr. Rita Sketerskienė
2020-05-26

2020-05-22
Higienos instituto direktorius
...igijus Jankauskas

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. rugsėjo 28 d. įsakymu Nr. V-1082
(Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. birželio 8 d. įsakymo Nr. V-1399 redakcija)

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

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

2. Informacijos tvarkymo taisyklės parengtos 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“ ir 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“.

3. Informacinės sistemos duomenų bazėje tvarkomi Informacinės sistemos duomenys, nurodyti Vaikų sveikatos stebėsenos informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos nuostatai) 15–17 punktuose.

4. 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“, 8.1 ir 8.2 papunkčiais, Informacinėje sistemoje tvarkoma informacija, kuri priskiriama prie svarbios informacijos kategorijos.

5. Informacijos tvarkymo taisyklės privalomos Informacinės sistemos valdytojui, Informacinės sistemos tvarkytojui, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui bei saugos įgaliotiniui. Už Informacijos tvarkymo taisyklių įgyvendinimo

2020 -05- 22

organizavimą ir kontrolę atsako Informacinės sistemos saugos įgaliotinis. Už Informacinės sistemos elektroninės informacijos tvarkymą atsakingi:

5.1. Informacinės sistemos naudotojai, dirbantys Higienos institute, – už duomenų, nurodytų Informacinės sistemos nuostatų 17 punkte, tvarkymą;

5.2. Informacinės sistemos visuomenės sveikatos specialistai – už duomenų, nurodytų Informacinės sistemos nuostatų 15, 16 punktuose, tvarkymą;

5.3. Informacinės sistemos administratorius – už duomenų, nurodytų Informacinės sistemos nuostatų 15–17 punktuose, tvarkymą, už Informacinės sistemos administravimą, duomenų bazių atkūrimą ir priežiūrą, prieinamumo užtikrinimą, klasifikatorių tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Kompiuterinės įrangos saugos priemonės turi atitikti reikalavimus:

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

6.2. Informacinės sistemos tarnybinėse stotyse ir Higienos instituto (toliau – Informacinės sistemos tvarkytojo) kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti;

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

6.4. Informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei 12 valandų;

6.5. vidinių informacinės sistemos naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga. Informacinės sistemos saugos įgaliotinis turi parengti, su Informacinės sistemos valdytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

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

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

6.8. patekimas prie Informacinės sistemos naudotojų darbo vietų yra kontroliuojamas: stacionariais kompiuteriais, turinčiais prieigą prie Informacinės sistemos, galima naudotis tik Informacinės sistemos tvarkytojo patalpose;

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

6.10. svarbiausia kompiuterinė įranga dubliuojama, jos techninė būklė nuolat stebima;

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

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

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

7.2. 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.

2020 -05- 22

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

7.4. Informacinės sistemos tarnybinėse stotyse įrašomi ir saugomi duomenys apie Informacinės sistemos tarnybinių stočių ir taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Informacinės sistemos tarnybinėse stotyse, kitus saugai svarbius įvykius, nurodant naudotojo identifikatorių ir įvykio laiką. Šie duomenys analizuojami ne rečiau kaip kartą per savaitę;

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

7.6. programinei įrangai testuoti naudojama atskira testavimo aplinka;

7.7. Informacinės sistemos tinkle įdiegtos automatinės įsilaužimo aptikimo sistemos;

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

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

8.1. Informacinės sistemos tarnybinės stotys, Informacinės sistemos tvarkytojo naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai reguliariai analizuojami;

8.2. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas užtikrinamas naudojant šifravimą, virtualų privatų tinklą (VPN), skirtines linijas, saugų elektroninių ryšių tinklą;

8.3. Informacinės sistemos programinė įranga 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*);

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

8.5. prisijungimai viešaisiais ryšių tinklais prie Informacinės sistemos leidžiami tik iš nustatytų IP adresų;

8.6. nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas protokolu, skirtu duomenų šifravimui;

8.7. 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;

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

9. Patalpų ir aplinkos saugumo užtikrinimo priemonės turi atitikti reikalavimus:

9.1. patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės;

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

9.3. veikia patekimo į patalpas kontrolės sistema;

9.4. patalpose naudojami nepertraukiamo elektros maitinimo šaltiniai;

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

10. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

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

2020 -05- 22

10.2. kiekvienas naudotojas, prieš naudodamasis Informacine sistema, savo tapatybę patvirtina slaptažodžiu;

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

10.4. baigus darbą imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama, uždaroma programinė įranga, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą;

10.5. 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;

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

10.7. išorinėje duomenų laikmenoje teikiami asmens duomenys ir sveikatos asmens duomenys šifruojami arba naudojamos kitos saugos priemonės, užtikrinančios, kad asmens duomenys ir sveikatos asmens duomenys bus perduoti saugiai ir nebus galimybės tretiesiems asmenims jais pasinaudoti;

10.8. išoriniais duomenų perdavimo tinklais perduodami asmens duomenys ir sveikatos asmens duomenys šifruojami;

10.9. saugos atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

10.10. per metus turi būti užtikrintas Informacinės sistemos prieinamumas: ne mažiau kaip 96 proc. laiko visą parą.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

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

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

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

11.4. 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 nei 1 metus.

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

12.1. 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;

12.2. 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;

2020 -05- 22

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

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

13.1. 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;

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

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

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

14. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

14.1. Informacinės sistemos naudotojai, pastebėję neteisėtos veiklos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informacinės sistemos administratoriui;

14.2. 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, siekiant nustatyti neteisėtos veiklos šaltinį, laiką ir veiksmus;

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

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

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

15.2. pokyčių projektavimą ir kūrimą atlieka Higienos instituto direktoriaus 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;

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

15.4. 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;

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

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

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

2020 -05- 22

15.8. 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;

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

16. Nešiojamųjų kompiuterių naudojimo tvarka:

16.1. nešiojamieji kompiuteriai skirti savivaldybių visuomenės sveikatos biurų specialistams, tvarkantiems Informacinės sistemos duomenis, nurodytus Informacinės sistemos Nuostatų 15, 16 punktuose;

16.2. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

16.3. nešiojamųjų kompiuterių nenaudojant, jie turi būti saugomi saugioje vietoje.

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

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

18. 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.

19. 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.

20. 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“.

21. 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.

22. 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.

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Basa Sinkevičiūtė
2020-06-05

Teisės skyriaus vyriausiasis specialistas
Narimantas Satkus
2020-06-09

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-22

Sveikatos saugos skyriaus vedėja
Dr. Rita Skeferskienė
2020-05-26

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vedėja
Vilma Telyčėnienė
2020 05 27

2020-05-28

Higienos instituto direktorius
Remigijus Jankauskas

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2015 m. rugsėjo 28 d.
įsakymu Nr. V-1082
(Lietuvos Respublikos sveikatos apsaugos
ministro 2020 m. birželio 8 d. įsakymo Nr. V-1399
redakcija)

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Vaikų sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plane (toliau – Veiklos tęstinumo valdymo planas) aprašomos procedūros, kurių būtina laikytis atkuriant Vaikų sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) veiklą įvykus elektroninės informacijos saugos ir (ar) kibernetiniam incidentui (toliau – saugos incidentas).

2. Veiklos tęstinumo valdymo planas vykdomas įvykus elektroninės informacijos saugos incidentui, kuris gali sudaryti neteisėto prisijungimo prie Vaikų sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) 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 neteisėtai panaudoti.

3. Veiklos tęstinumo valdymo plano reikalavimai privalomi Informacinės sistemos valdytojui, Informacinės sistemos tvarkytojui, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui bei saugos įgaliotiniui, asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas).

4. 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).

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

6. 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.

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

2020 -05- 22

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

8. Veiklos tęstinumo valdymo grupės sudėtis:

8.1. vadovas – Higienos instituto Sveikatos informacijos centro vadovas;

8.2. vadovo pavaduotojas – Higienos instituto Sveikatos informacijos centro Registrų skyriaus Vaikų sveikatos stebėsenos informacinės sistemos valdymo specialistas;

8.3. nariai:

8.3.1. Higienos instituto Bendrųjų reikalų skyriaus vadovas;

8.3.2. Informacinės sistemos saugos įgaliotinis;

8.3.3. kibernetinio saugumo vadovas.

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

9.1. analizuoja saugos incidentus ir priima sprendimus Informacinės sistemos veiklos tęstinumo valdymo klausimais;

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

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

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

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

9.6. organizuoja darbuotojų, Informacinės sistemos techninės įrangos gabenimą;

9.7. vykdo Informacinės sistemos veiklos atkūrimo priežiūrą ir koordinuoja veiklos atkūrimo veiksmus, taip pat vykdo kitas jai pavestas funkcijas.

10. Veiklos atkūrimo grupės sudėtis:

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

10.2. vadovo pavaduotojas – Informacinės sistemos administratorius;

10.3. nariai:

10.3.1. Informacinės sistemos saugos įgaliotinis;

10.3.2. Higienos instituto Registrų skyriaus specialistas.

11. Veiklos atkūrimo grupė vykdo šias funkcijas:

11.1. organizuoja Informacinės sistemos tarnybinių stočių veikimo atkūrimą;

11.2. organizuoja Informacinės sistemos pagrindinio tvarkytojo kompiuterių tinklo veikimo atkūrimą;

11.3. organizuoja Informacinės sistemos elektroninės informacijos atkūrimą;

11.4. organizuoja taikomųjų programų tinkamo veikimo atkūrimą;

11.5. organizuoja Informacinės sistemos tvarkytojo darbuotojų kompiuterių veikimo atkūrimą ir Informacinės sistemos naudotojų prijungimą prie kompiuterių tinklo;

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

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

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

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

2020 -05- 22

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

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

16. Veiklos atkūrimo grupės vadovas nuolat informuoja Veiklos tęstinumo valdymo grupę apie Informacinės sistemos veiklos atkūrimo eigą.

17. Veiklos tęstinumo valdymo ir Veiklos atkūrimo grupių nariai turi reaguoti ir valdyti saugos incidentus, vadovaudamiesi 1 priede pateiktomis instrukcijomis.

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

19. Įvykus saugos incidentui:

19.1. 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;

19.2. 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;

19.3. 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 Veiklos tęstinumo valdymo plano 2 priede nustatyta tvarka;

19.4. 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;

19.5. Informacinės sistemos saugos įgaliotinis įrašo informaciją apie saugos incidentą į Vaikų sveikatos stebėsenos informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalą (Veiklos tęstinumo valdymo plano 3 priedas), vadovauja Vaikų sveikatos stebėsenos informacinės sistemos veiklos atkūrimo detaliajame plane nurodytiems veiksmams;

19.6. 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;

19.7. 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;

19.8. 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;

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

20. Elektroninės informacijos saugos incidentai registruojami Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnale (3 priedas), už kurio pildymą atsakingas Informacinės sistemos administratorius.

2020 -05- 22

21. Įvykus saugos incidentui, Informacinės sistemos veikla atkuriama atsarginėse Higienos instituto patalpose, Didžioji g. 22, Vilniuje, kurios atitinka Vaikų sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse tarnybinių stočių patalpoms nurodytus reikalavimus.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

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

22.1. Vaikų sveikatos stebėsenos informacinės sistemos 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 Vaikų sveikatos stebėsenos informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir 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 keliamų reikalavimų lygį;

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

22.3. Informacinės sistemos programinės įrangos priežiūros ir Virtualių serverių nuomos sutarčių kopijos;

22.4. 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;

22.5. 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;

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

23. Veiklos tęstinumo valdymo plano 22 punkte nurodytų dokumentų, susegtų į bylą, kopijas saugo Informacinės sistemos Veiklos atkūrimo grupės vadovas.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

24. Plano veiksmingumo išbandymą organizuoja Informacinės sistemos saugos įgaliotinis.

25. Plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus.

26. Prieš įdiegiant naujus Informacinės sistemos komponentus, pradedant teikti naujas paslaugas arba pasikeitus Informacinės sistemos veiklos aplinkai, Informacinės sistemos saugos įgaliotinis turi peržiūrėti Planą ir, esant reikalui, atlikti neeilinį Plano veiksmingumo išbandymą.

27. Plano veiksmingumas turi būti išbandomas simuliavimo būdu pagal saugos incidento situacijos scenarijų.

28. Išbandžius Plano veiksmingumą, Informacinės sistemos saugos įgaliotinis turi parengti Plano veiksmingumo išbandymo ataskaitą ir pateikti ją Informacinės sistemos valdytojui. Plano veiksmingumo išbandymo ataskaitos forma pateikta 4 priede.

2020 -05- 2

29. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Rasa Sinkevičiūtė
2020-06-05

Teisės skyriaus vyriausiasis specialistas
Narimantas Satkus
2020-06-04

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vedėja
Ilma Telyčėnienė
2020-05-27

Elektroninės sveikatos sistemos ir informacinių išteklių skyriaus vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-28

Sveikatos saugos skyriaus vedėja
Dr. Rita Sketerskienė
2020-05-26

2020-05-22
Higienos instituto direktorius
Remigijus Jankauskas

Vaikų sveikatos stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
1 priedas

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
1. Oro sąlygos (smarkus lietus, labai smarki audra, viesulas, škvalas, kruša, žemės drebėjimas, smarkus speigas)	1.1. Elektroninės informacijos saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Vaikų sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) saugos įgaliotinis, Informacinės sistemos administratorius
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		1.1.3. Priemonių plano įgyvendinimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
	1.2. Darbuotojų elektroninės informacijos saugos incidento pasekmėms likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		1.2.2. Žalą likviduojančių darbuotojų veiksmų koordinavimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
	1.3. Oro prognozės sekimas	1.3.1. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius

2020-05-22

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
	1.4. Rekomendacijų teikimas darbuotojams, dirbantiems pavojaus vietoje	1.4.1. Elektroninės informacijos saugos incidento pasekmes likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		1.4.2. Darbuotojų informavimas apie elgseną pavojaus vietoje	Informacinės sistemos saugos įgaliotinis
		1.4.3. Pirmosios pagalbos suteikimo organizavimas nukentėjusiems darbuotojams	Informacinės sistemos saugos įgaliotinis
		1.4.4. Nukentėjusių darbuotojų gabenimo į gydymo įstaigą organizavimas	Informacinės sistemos saugos įgaliotinis
	1.5. Pavojaus vietų ženklinimas	1.5.1. Darbuotojų informavimas 1.5.2. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
2. Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei gauta rekomendacija	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		2.1.2. Galimybių evakuoti darbuotojus paieška, jei yra rekomenduojama tai padaryti	Informacinės sistemos saugos įgaliotinis
	2.2. Darbuotojų evakavimas (pagal priešgaisrinės gelbėjimo tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Informacinės sistemos saugos įgaliotinis
	2.3. Darbas pavojaus zonoje	2.3.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Informacinės sistemos saugos įgaliotinis
	2.4. Komunikacijų, sukeliančių pavojų, išjungimas. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.4.1. Priešgaisrinės gelbėjimo tarnybos nurodymų vykdymas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius

2020 -05- 22

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
3. Patalpų užgrobimas	3.1.Teisėsaugos institucijų informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos institucijos rekomendacijos	Informacinės sistemos saugos įgaliotinis
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei gauta rekomendacija	Informacinės sistemos saugos įgaliotinis
	3.2. Darbuotojų evakavimas, jei yra rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	Informacinės sistemos saugos įgaliotinis
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos institucijos nurodymų vykdymas	Informacinės sistemos saugos įgaliotinis
	3.4. Teisėsaugos institucijos nurodymų vykdymas, jei yra rekomendacijų	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Informacinės sistemos saugos įgaliotinis
	3.5. Veiksmai išlaisvinus užgrobtas patalpas	3.5.1. Padarytos žalos įvertinimas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius
		3.5.3. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos administratorius
4. Patalpai padaryta žala arba patalpos praradimas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.1. Suinteresuotos tarnybos rekomendacijų dėl galimybės dirbti pavojaus zonoje gavimas	Informacinės sistemos saugos įgaliotinis
		4.1.2. Darbuotojų informavimas apie rekomendacijas	Informacinės sistemos saugos įgaliotinis
	4.2. Informacinės sistemos įrangos perkėlimas į atsargines patalpas	4.2.1. Darbuotojų informavimas apie darbą patalpose	Informacinės sistemos saugos įgaliotinis
5. Energijos tiekimo sutrikimai	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas, tarnybinių stočių, kitos techninės įrangos energijos maitinimo išjungimas	5.1.1 Sutrikimų šalinimo organizavimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis

2020 -05- 2 2

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
	5.2. Kreipimasis į energijos tiekimo įmonę dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	5.2.1. Rekomendacijų iš energijos tiekimo įmonės gavimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
	5.3. Sutrikimų pašalinimas	5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
		5.3.2. Padarytos žalos įvertinimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
		5.3.3. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis
6. Vandentiekio ir šildymo sistemos sutrikimai	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	6.1.1. Vandentiekio ar šildymo paslaugų teikėjų paklausimas dėl leidimo dirbti ir rekomendacijų gavimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
		6.1.2. Darbuotojų informavimas apie rekomendacijas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
	6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.2.1. Padarytos žalos įvertinimas, sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
		6.2.2. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis
7. Ryšio sutrikimai	7.1. Ryšio sutrikimo priežasčių nustatymas	7.1.1. Kreiptis į ryšio paslaugos teikėją	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis

2020 -05- 22

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
	7.2. Ryšio paslaugų teikėjo informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.2.1. Nustatyti ir įgyvendinti priemones, apsaugančias nuo ryšio sutrikimų pasikartojimo	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis
	7.3. Sutrikimo pašalinimas	7.3.1. Kreiptis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas	Informacinės sistemos administratorius
8. Tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas	8.1. Pranešti teisėsaugos institucijai, draudimo bendrovei apie įvykį	8.1.1. Darbuotojų saugos incidento pasekmėms likviduoti paskyrimas, instruktavimas, jų veiksmų nustatymas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
	8.2. Elektroninės informacijos saugos incidento pasekmių šalinimas	8.2.1. Kreiptis į įrangos tiekėjus dėl įrangos remonto ar naujos įrangos įsigijimo	Informacinės sistemos administratorius
		8.2.2. Įsigytos įrangos diegimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
9. Programinės įrangos sugadinimas, praradimas	9.1. Saugos incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	9.1.1. Saugos incidento metu padarytos žalos įvertinimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas

2020-05-22

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
	9.2. Darbuotojų saugos incidento pasekmėms likviduoti paskyrimas, žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
		9.2.2. Kreipimasis į teisėsaugos institucijas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
10. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas	10.1. Saugos incidento pasekmių įvertinimas	10.1. Prarastų, iškraipytų ar sunaikintų Informacinės sistemos duomenų ir dokumentų atkūrimas	Informacinės sistemos administratorius
		10.2. Prarastų, iškraipytų ar sunaikintų Informacinės sistemos duomenų ir dokumentų atkūrimo kontrolė	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas
11. Darbuotojų praradimas	11.1. Saugos incidento pasekmių įvertinimas	Trūkstamų darbuotojų paieška ir priėmimas į darbą	Informacinės sistemos administratorius, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos tvarkytojo kibernetinio saugumo vadovas

Teisės skyriaus vyriausiasis specialistas Narimantas Satkus 2020-06-04

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė Rasa Sinkevičiūtė 2020-06-05

Elektroninės sveikatos sistemos informacinių išteklių skyriaus vedėja Vilma Telyčėnienė 2020-05-27

Sveikatos saugos skyriaus vedėja Dr. Rita Skeferskienė 2020-05-26

2020-05-27

Higienos instituto direktorius Remigijus Jankauskas

Vaikų sveikatos stebėsenos
informacinės sistemos veiklos
tęstinumo valdymo plano
2 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO IR PRANEŠIMO APIE KIBERNETINIUS INCIDENTUS TVARKOS APRAŠAS

1. Kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro informavimo tvarkos aprašas reglamentuoja kibernetinių incidentų valdymo ir pranešimo apie kibernetinius incidentus tvarką.

2. Nacionaliniam kibernetinio saugumo centrui (toliau – Centras) pranešama apie Informacinėje sistemoje įvykusius:

2.1. didelės reikšmės kibernetinį incidentą – ne vėliau kaip per vieną valandą nuo jo nustatymo;

2.2. vidutinės reikšmės kibernetinį incidentą – ne vėliau kaip per keturias valandas nuo jo nustatymo;

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

3. Pranešime apie didelės ir vidutinės reikšmės kibernetinį incidentą nurodoma:

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

3.2. trumpas kibernetinio incidento apibūdinimas;

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

3.4. kibernetinio incidento kategorija;

3.5. kibernetinio incidento šalinimo tvarka (nurodoma, ar tai prioritetas, ar ne).

3.6. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

4. Pranešime apie nereikšmingą kibernetinį incidentą pateikiama apibendrinta informacija apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

5. Centrui pateikiama kibernetinio incidento tyrimo ataskaita apie:

5.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

5.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

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

6. Centrui teikiant didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitą nurodoma Informacinės sistemos valdytojui ir (ar) tvarkytojui žinoma informacija:

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

6.2. Informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (informacinė sistema, elektroninių ryšių tinklas, tarnybinė stotis ir panašiai);

6.3. kibernetinio incidento veikimo trukmė;

6.4. kibernetinio incidento šaltinis;

6.5. kibernetinio incidento požymiai;

6.6. kibernetinio incidento veikimo metodas;

6.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

2020 -05- 22

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

6.9. kibernetinio incidento būsena (aktyvus, pasyvus);

6.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

6.11. galimos kibernetinio incidento valdymo priemonės;

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

7. Įvertinus, kad negalima savarankiškai ištirti ar suvaldyti kibernetinio incidento per dvylika valandų, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo, turi būti kreiptasi pagalbos į Centrą.

8. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinių sistemų veikla, atitinkanti Vaikų sveikatos stebėsenos informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“, nustatytus reikalavimus.

9. Ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo turi būti informuojami ryšių ir informacinės sistemos teikiamų paslaugų gavėjai, jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir informacinės sistemos teikiamų paslaugų gavėjui.

10. Tais atvejais, kai Centro nurodymu toliau tiriamas ir valdomas pavojingas kibernetinis incidentas, ne rečiau kaip kas keturias valandas teikiama Centrui atnaujinta informacija apie pavojingo kibernetinio incidento valdymo būklę, kurią sudaro Nacionalinio kibernetinių incidentų valdymo plano 24 punkte nurodyta informacija.

11. Centrui perėmus tirti ir (ar) organizuoti pavojingo kibernetinio incidento valdymą, privaloma:

11.1. nuolat rinkti, apdoroti informaciją, susijusią su kibernetiniu incidentu, ir ne rečiau kaip kas keturias valandas ją teikti Centrui;

11.2. ne rečiau kaip kas keturias valandas teikti Centrui informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus, kurią sudaro Nacionalinio kibernetinių incidentų valdymo plano 24 punkte nurodyta informacija;

11.3. vykdyti Centro nurodymus, susijusius su kibernetinio incidento tyrimu ir (ar) valdymo organizavimu, ir dalyvauti kibernetinio incidento valdymo procese, taikydami kibernetinio saugumo užtikrinimo priemones.

12. 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, tubi tūi imtasi veiksmų, reikalingų kibernetiniam incidentui nustatyti ir patvirtinti. Nenustačius kibernetinio incidento požymių, ne vėliau kaip per keturias valandas nuo pranešimo apie kibernetinį incidentą gavimo turi būti informuojamos KIVT institucijos.

13. Nacionalinio kibernetinių incidentų valdymo plane nurodyta informacija, susijusi su kibernetiniais incidentais ir jų valdymu, turi būti perduodama per kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis.

14. Po kibernetinio incidento suvaldymo ar pasibaigimo turi būti atlikta jo analizė. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

15. Ištyrus Informacinėje sistemoje įvykusį kibernetinį incidentą, turi būti išanalizuota ir įvertinta visa informacija, susijusi su kibernetiniu incidentu, atlikti veiksmai ir panaudotos priemonės:

15.1. ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikiami kibernetinio incidento analizės rezultatai Centrui ir kibernetinio saugumo

2020 -05- 22

informaciniame tinkle paskelbiama susisteminta ir aktuali neįslaptinta informacija apie kibernetinio incidento nustatymą ir suvaldymą;

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

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

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

16. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami konkrečiai kategorijai, nustatyti Nacionalinio kibernetinių incidentų valdymo plano priede.

...umentų valdymo ir
...asmenų priėmimo skyriaus
vyriausioji specialistė
Rasa Sinkevičiūtė
2020-06-05

Elektroninės sveikatos sistemos
ir informacinių išteklių skyriaus
vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-28

Teisės skyriaus
vyriausiasis specialistas
Narimantas Satkus
2020-06-04

Sveikatos saugos skyriaus vedėja
Dr. Rita Skeferskienė
2020-05-26

Elektroninės sveikatos sistemos
ir informacinių išteklių skyriaus vedėja
2020-06-22
Vilma Telyčėnienė

2020-05-22
Higienos instituto direktorius
Remigijus Jankauskas

Vaikų sveikatos stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
3 priedas

(Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalo forma)

VAIKŲ 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 – įsilaužimas į vidinį kompiuterių tinklą; 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 – nešiojamųjų kompiuterių ir juose saugomų duomenų praradimas; 11 – pavojingas (įtartinas) radinys; 12 – kompiuterių virusų, nepageidautinų laiškų (*spam*) atakos; 13 – dokumentų praradimas; 14 – duomenų iš duomenų teikėjų negavimas; 15 – dalinis Informacinės sistemos sutrikimas dėl neaiškių priežasčių; 16 – gamtos reiškiniai.

Dokumentų valdymo ir asmenų priėmimo skyriaus vyriausioji specialistė
Rasa Sinkevičiūtė
2020-05-27

Elektroninės sveikatos sistemos ir informacinių išteklių skyrius
vyriausiasis specialistas
Vytautas Gaveniavas
2020-05-27

Elektroninės sveikatos sistemos ir informacinių išteklių skyrius
Vilma Telyčėnė
2020-05-27

Teisės skyriaus vyriausiasis specialistas
Narimantas Satkus
2020-05-26

Sveikatos saugos skyriaus vedėja
Dr. Rita Skeferskienė
2020-05-26

2020-05-22
Higienos instituto direktorius
Remigijus Jankauskas

Vaikų sveikatos stebėsenos
informacinės sistemos
veiklos tęstinumo valdymo plano
4 priedas

(Vaikų sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano išbandymo ataskaitos forma)

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO ATASKAITA

(Grupės susitikimo data)

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 veiklos tęstinumo valdymo planą:

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

Elektroninės sveikatos sistemos
ir informacinių išteklių skyriaus
vyriausiasis specialistas
Vytautas Gavėnavičius
2020-05-28

Teisės sky
vyriausiasis sp
Natalija
2020-05-27

Dokumentų valdymo, sveikatos saugos skyriaus vedėja
priėmimo skyriaus
vyriausioji specialistė
Dr. Rita Sketerskienė
2020-05-26

Rasa Sinkevičiūtė
2020-06-05

2020-05-27
instituto direktorius
Junkauskas