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

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,

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.

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.

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

_____

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

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

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

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai
6. Vandentiekio ir šildymo sistemos sutrikimai	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
	6.1. 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

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

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

_____

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;

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

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.

_____

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.

_____

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)

_____