PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2021 m. rugpjūčio 30 d. įsakymu Nr.V-1959

SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINIS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Sveikatos priežiūros įstaigos (toliau – SPĮ) valdomos ir tvarkomos informacinės sistemos (toliau – IS) veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja SPĮ IS veiklos tęstinumo užtikrinimą.

2. Plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ ir Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas).

3. Planas parengtas pagrindinio IS tvarkytojo (toliau – tvarkytojas) patalpoms, esančioms _____ (nurodomas adresas), kuriose yra pagrindinė IS informacinių technologijų infrastruktūra, reikalinga IS veiklai. IS komponentų, kurie yra IS kitų tvarkytojų (toliau – tvarkytojai) organizacijose, veiklos tęstinumo valdymą ir veiklos atkūrimą reglamentuoja IS kitų tvarkytojų veiklos tęstinumo valdymą reglamentuojantys dokumentai.

4. Planas įsigalioja įvykus elektroninės informacijos saugos (kibernetiniam) incidentui, dėl kurio IS tvarkytojas (tvarkytojai) negali teikti IS elektroninių paslaugų daliai arba visiems IS naudotojams ir būtina atkurti įprastą IS veiklą IS tvarkytojo (tvarkytojų) patalpose arba atsarginėse patalpose. Plano vykdymą atitinkamai inicijuoja IS tvarkytojo (tvarkytojų) paskirti atsakingi asmenys. Plano nuostatos taip pat taikomos po stichinės nelaimės, avarijos ar kitų ekstremalių situacijų, kai būtina atkurti įprastą IS veiklą.

5. Įvykus kibernetiniam incidentui vadovaujamasi Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Nutarimu.

6. Kibernetinių ir elektroninės informacijos saugos incidentų tyrimas atliekamas vadovaujantis IS tvarkytojo (tvarkytojų) patvirtintais teisės aktais, reglamentuojančiais kibernetinių ir elektroninės informacijos saugos incidentų valdymo veiksmus IS tvarkytojo (tvarkytojų) įstaigose.

7. Identifikavus kibernetinį incidentą, atliekamas incidento vertinimas pagal poveikį ir incidento priskyrimas vienai iš šių kategorijų: didelio, vidutinio ar nereikšmingo. Kriterijai, pagal kuriuos incidentas priskiriamas tam tikrai kategorijai, yra nurodyti Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Nutarimu.

8. Atsakingų asmenų įgaliojimai įvykus kibernetiniam ar elektroninės informacijos saugos incidentui:

8.1. IS tvarkytojo (tvarkytojų) paskirti saugos įgaliotiniai turi:

8.1.1. bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, kibernetinius ir (ar) elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su kibernetiniais ir (ar) elektroninės informacijos saugos incidentais IS tvarkytojo (tvarkytojų) organizacijose ir (arba) IS komponentuose, už kurių tvarkymą jie yra atsakingi savo organizacijose, išskyrus tuos atvejus, kai šią funkciją atlieka IS tvarkytojo (tvarkytojų) sudarytos elektroninės informacijos saugos ir kibernetinio saugumo darbo grupės;

8.1.2. duoti privalomus vykdyti nurodymus ir pavedimus IS valdytojo ir IS tvarkytojo (tvarkytojų) darbuotojams, jeigu tai būtina elektroninės informacijos saugos ir kibernetinio saugumo politikai įgyvendinti;

8.1.3. koordinuoti kibernetinių ir elektroninės informacijos saugos incidentų tyrimą;

8.2. IS administratorius (toliau – administratorius) turi:

8.2.1. dalyvauti atliekant Plano 17 punkte nurodytas funkcijas;

8.2.2. vykdyti kitus Plane ir Plano priede nurodytus veiksmus ir IS veiklos tęstinumo valdymo grupės (toliau – Veiklos tęstinumo valdymo grupė) ir IS veiklos atkūrimo grupės (toliau – Veiklos atkūrimo grupė) pavestas užduotis;

8.3. IS naudotojai vykdo Veiklos tęstinumo valdymo grupės nurodymus.

9. Nurodomi asmenys, atsakingi už kibernetinių incidentų tyrimą ir pranešimą apie kibernetinius incidentus kompetentingoms institucijoms: Nacionaliniam kibernetinio saugumo centrui, Valstybinei duomenų apsaugos inspekcijai, Lietuvos policijai, taip pat būdai, kuriais pranešama apie kibernetinį incidentą kompetentingoms institucijoms (pvz., Nacionaliniam kibernetinio saugumo centrui pranešama užpildant specialią formą interneto svetainėje www.nksc.lt, rašant el. paštu cert@nksc.lt arba skambinant trumpuoju numeriu 1843).

10. Planas privalomas IS valdytojui, IS tvarkytojui (tvarkytojams), saugos įgaliotiniams, IS duomenų valdymo įgaliotiniams, administratoriams, IS naudotojams, IS techninės ir programinės įrangos priežiūros funkcijas teikiantiems paslaugų teikėjams, jei tokios funkcijos paslaugų teikėjams perduotos Valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka.

11. Įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, dėl kurio IS tvarkytojas (tvarkytojai) negali teikti IS elektroninių paslaugų daliai arba visiems IS naudotojams ir būtina atkurti įprastą IS veiklą IS tvarkytojo (tvarkytojų) patalpose arba atsarginėse patalpose, veiklai atkurti naudojami IS valdytojo ir IS tvarkytojo (tvarkytojų) finansiniai ir kitokie ištekliai.

12. IS veiklos kriterijai, pagal kuriuos nustatoma, ar IS veikla atkurta:

12.1. IS priima elektroninę informaciją iš registrų ir IS, elektroninės informacijos teikėjų;

12.2. IS elektroninė informacija nuolat atnaujinama ir išsaugoma;

12.3. užtikrintas IS elektroninės informacijos vientisumas ir konfidencialumas;

12.4. IS elektroninė informacija nuolat teikiama IS naudotojams, registrams ir kitoms informacinėms sistemoms;

12.5. užtikrintas IS prieinamumas – ne mažiau kaip ___ proc. laiko visą parą (IS neprieinamumo bendra trukmė per metus valandomis – iki ___ val.).

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

13. IS veiklos tęstinumui užtikrinti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui sudaromos Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė. Veiklos tęstinumo valdymo grupės vadovas ir Veiklos atkūrimo grupės vadovai turi teisę į šių grupių veiklą pasitelkti ir kitus IS valdytojo ir IS tvarkytojo (tvarkytojų) darbuotojus ar trečiosios šalies kompetentingus specialistus, jeigu tai būtina IS veiklai atkurti ir (ar) IS veiklos tęstinumui užtikrinti.

14. Veiklos tęstinumo valdymo grupės sudėtis:

14.1. Veiklos tęstinumo valdymo grupės vadovas: _____;

14.2. Veiklos tęstinumo valdymo grupės vadovo pavaduotojas: _____;

14.3. Veiklos tęstinumo valdymo grupės nariai: _____ (nurodomi Veiklos tęstinumo valdymo grupės nariai).

15. Veiklos tęstinumo valdymo grupės funkcijos:

15.1. situacijos analizė ir sprendimų IS veiklos tęstinumo valdymo klausimais priėmimas;

15.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

15.3. bendravimas su kitų registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

15.4. bendravimas su teisėsaugos ir kitomis institucijomis, šių institucijų darbuotojais ir kitomis interesų grupėmis;

15.5. finansinių ir kitų išteklių, reikalingų IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, naudojimo kontrolė;

15.6. elektroninės informacijos fizinės saugos organizavimas įvykus elektroninės informacijos saugos ar kibernetinio saugumo incidentui;

15.7. logistika (asmenų, daiktų, įrangos gabenimo organizavimas).

16. Veiklos atkūrimo grupės sudėtis:

16.1. Veiklos atkūrimo grupės vadovas: _____;

16.2. Veiklos atkūrimo grupės vadovo pavaduotojas: _____;

16.3. Veiklos atkūrimo grupės nariai:_____ (nurodomi Veiklos atkūrimo grupės nariai).

17. Veiklos atkūrimo grupės funkcijos:

17.1. tarnybinių stočių veikimo atkūrimo organizavimas;

17.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

17.3. IS elektroninės informacijos atkūrimo organizavimas;

17.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

17.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas.

18. Personalinę Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės sudėtį tvirtina pagrindinio IS tvarkytojo vadovas.

19. Veiklos tęstinumo valdymo grupės, Veiklos atkūrimo grupės veiklą organizuoja ir koordinuoja šių grupių vadovai.

20. Veiksmai, reikalingi IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, jų vykdymo eiliškumas, terminai ir atsakingi vykdytojai nurodyti Plano priede nustatytame IS veiklos atkūrimo detaliajame plane.

21. Atsarginėms patalpoms, naudojamoms IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, keliami šie reikalavimai:

21.1. turi atitikti priešgaisrinės saugos reikalavimus;

21.2. turi atitikti IS techninės įrangos gamintojų nustatytus reikalavimus įrangos darbo aplinkai (pavyzdžiui, tinkama oro temperatūra, oro drėgmė ir kita);

21.3. turi būti įrengtos langų, durų, IS techninės įrangos, kabelių fizinės apsaugos priemonės;

21.4. turi būti įrengta patalpų apsaugos signalizacija, kurios signalai turi būti persiunčiami patalpas saugančiai saugos tarnybai;

21.5. turi būti atskirtos nuo bendrojo naudojimo patalpų;

21.6. turi būti interneto ryšio prieiga;

21.7. turi būti įrengti nenutrūkstamą elektros tiekimą užtikrinantys maitinimo šaltiniai;

21.8. turi būti užtikrintas elektroninių ryšių tinklais perduodamos elektroninės informacijos vientisumas ir konfidencialumas;

21.9. turi būti įdiegtos kitos priemonės, atitinkančios pagrindinėms patalpoms keliamus reikalavimus.

22. Atsarginės patalpos, pritaikytos IS atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, yra _____ patalpos, esančios _____. Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė organizuoja bendrą susirinkimą, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, nenumatytoms situacijoms arba įvykus esminiams organizaciniams IS ar jų komponentų pokyčiams.

23. Veiklos tęstinumo valdymo grupė, atlikusi situacijos analizę, informuoja Veiklos atkūrimo grupę apie priimtus sprendimus IS veiklos tęstinumo valdymo klausimais. Veiklos atkūrimo grupė, atsižvelgdama į priimtus sprendimus, organizuoja IS veiklos atkūrimą.

24. Veiklos tęstinumo valdymo ir Veiklos atkūrimo grupės tarpusavyje bendrauja žodžiu, telefonu ir elektroniniu paštu.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

25. IS veiklos tęstinumui užtikrinti turi būti parengti ir saugomi šie dokumentai:

25.1. IS dokumentacija, kurioje nurodyta IS informacinių technologijų įranga ir jos parametrai, už ją atsakingi asmenys;

25.2. kiekvieno pastato, kuriame yra IS įranga, aukštų patalpų brėžiniai ir juose pažymėta:

25.2.1. tarnybinės stotys;

25.2.2. kompiuterių tinklo ir telefonų tinklo mazgai;

25.2.3. kompiuterių tinklo ir telefonų tinklo tiesimo tarp pastato aukštų vietos;

25.2.4. elektros įvedimo pastate vietos;

25.2.5. IS kompiuterių tinklo fizinio ir loginio sujungimo schemos.

25.3. kompiuterinės, techninės ir programinės įrangos sutarčių sąrašas;

25.4. elektroninės informacijos atsarginių kopijų darymo ir išbandymo tvarkos aprašas, kuriame turi būti nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

25.5. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, kuriais šiuos asmenis galima pasiekti bet kuriuo paros metu;

25.6. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos IS valdytojo ir tvarkytojo (tvarkytojų) poreikius atitinkančiai IS veiklai užtikrinti, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui ar nenumatytai situacijai, specifikacija; už šios įrangos priežiūrą atsakingų administratorių sąrašas ir minimalūs reikiamos kompetencijos ar žinių lygio reikalavimai IS veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą;

25.7. elektroninės informacijos teikimo sutarčių sąrašas.

26. Už Plano 25.1.–25.6. papunkčiuose nurodytų dokumentų parengimo organizavimą, saugojimą, nuolatinį atnaujinimą ir kompiuterinės, techninės ir programinės įrangos sutarčių vykdymo priežiūrą atsakingas IS administratorius. Šiame punkte nurodyti dokumentai saugomi išspausdinti _____. Jeigu naudojama IS įranga (pagal nuomos, panaudos ar kitas sutartis) priklauso trečiajai šaliai ir yra jos patalpose, sutarties su trečiąja šalimi kopija turi būti saugoma kartu su šiame punkte nurodytais dokumentais.

27. Už Plano 25.7. papunktyje nurodyto dokumento parengimą, saugojimą, nuolatinį atnaujinimą ir elektroninės informacijos teikimo sutarčių vykdymo priežiūrą pagal kompetenciją atsakingas ___ . Elektroninės informacijos teikimo sutarčių sąrašas saugomas išspausdintas _____ patalpose.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

28. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus teorinių ir (ar) praktinių mokymų metu, modeliuojant kibernetinį ar elektroninės informacijos saugos incidentą. Plano veiksmingumo išbandymas gali būti planinis arba neplaninis. Plano veiksmingumo išbandymą organizuoja saugos įgaliotiniai.

29. Plano veiksmingumo išbandymo rezultatai turi būti naudojami Planui atnaujinti. Nustačius Plano veiksmingumo trūkumų, rengiama pastebėtų Plano veiksmingumo trūkumų šalinimo ataskaita. Už Plano veiksmingumo trūkumų šalinimo ataskaitos parengimą ir pateikimą IS valdytojui atsakingi saugos įgaliotiniai.

30. Plano veiksmingumo išbandymo metu pastebėti Plano veiksmingumo trūkumai šalinami remiantis efektyvumo, ekonomiškumo, rezultatyvumo ir operatyvumo principais.

31. Veiklos tęstinumo valdymo procesams tobulinti turi būti nustatomi ir vertinami šie rodikliai:

31.1. IS neprieinamumas valandomis per metus;

31.2. IS veiklos atkūrimo, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, trukmė.

_____

Sveikatos priežiūros įstaigos informacinės sistemos veiklos tęstinumo valdymo plano priedas

SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINIS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

1. Sveikatos priežiūros įstaigos (toliau – SPĮ) valdomos ir tvarkomos informacinės sistemos (toliau – IS) veiklos atkūrimo detaliajame plane (toliau – Detalusis planas) nurodomi veiksmai, reikalingi SPĮ IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, jų vykdymo eiliškumas, terminai ir atsakingi vykdytojai.

2. Įsigaliojus SPĮ IS veiklos tęstinumo valdymo planui, Veiklos tęstinumo valdymo grupė informuoja IS naudotojus, susijusių registrų ir kitų informacinių sistemų tvarkytojus, kitus suinteresuotus asmenis apie IS veikimo sutrikimus. Informacija teikiama pagrindinio IS tvarkytojo interneto svetainėje, IS taikomosiose programose, kitomis priemonėmis (pavyzdžiui, raštu, elektroniniu paštu ir panašiai).

3. Veiklos atkūrimo grupė informacinių sistemų veiklą atkuria pagal šiuos IS funkcijų prioritetus:

3.1. tarnybinių stočių veikimo atkūrimas:

3.1.1. duomenų bazės veikimo atkūrimas;

3.1.2. taikomųjų programų veikimo atkūrimas;

3.2. kompiuterių tinklo veikimo atkūrimas;

3.3. elektroninės informacijos atkūrimas;

3.4. taikomųjų programų veikimo atkūrimas;

3.5. interneto ryšio atkūrimas;

3.6. pagrindinio IS tvarkytojo kompiuterinių darbo vietų veikimo atkūrimas;

3.7. kitų IS tvarkytojų kompiuterinių darbo vietų veikimo atkūrimas.

4. IS veiklos atkūrimo veiksmai, atsižvelgiant į kibernetinio ar elektroninės informacijos saugos incidento tipą ir mastą, veiklos atkūrimo veiksmų pobūdį, turi būti atlikti per kuo trumpesnį terminą, kuris neturi būti ilgesnis kaip __ valandos. IS veiklos atkūrimo detalūs veiksmai nurodyti 1 lentelėje.

1 lentelė

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
1.	1.1.	1.1.1.	
	1.2.	1.2.1.	
	1.3.	1.3.1.	

_____