Suvestinė redakcija nuo 2021-04-01

PATVIRTINTA
Valstybinės ligonių kasos
prie Sveikatos apsaugos
ministerijos direktoriaus
2020 m. vasario 14 d.
įsakymu Nr. 1K-45

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ IR RYŠIŲ TECHNOLOGIJŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų ir ryšių technologijų veiklos tęstinumo valdymo planas (toliau – Veiklos tęstinumo valdymo planas) reglamentuoja Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) ir teritorinių ligonių kasų (toliau – TLK, VLK ir TLK kartu toliau vadinamos ligonių kasomis) taisykles bei procedūras, kurių būtina laikytis atkuriant VLK valdomų informacinių sistemų (toliau – informacinės sistemos) veiklą ir užtikrinant jų funkcijų vykdymo tęstinumą, įvykus elektroninės informacijos saugos ar kibernetinio saugumo incidentui (toliau – saugos incidentas).

2. Veiklos tęstinumo valdymo planas parengtas vadovaujantis:

2.1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio gairių aprašu, patvirtintais 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“;

2.2. 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“;

2.3. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

Papunkčio pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

2.4. VLK valdomų informacinių sistemų duomenų saugos nuostatais, patvirtintais VLK direktoriaus 2017 m. gruodžio 6 d. įsakymu Nr. 1K-234 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo“ (toliau – Duomenų saugos nuostatai);

2.5. kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

2.6. Lietuvos standartais LST ISO/IEC 27002 (aktualios redakcijos) „Informacijos saugumo valdymo praktikos kodeksas“, LST ISO/IEC 27001 (aktualios redakcijos) „Informacijos saugumo valdymo sistemos. Reikalavimai “.

3. Veiklos tęstinumo valdymo plane vartojamos sąvokos:

3.1. **informacinės sistemos ir ryšių technologijos** – informacinės sistemos, programinė ir techninė įranga, infrastruktūra ir kiti informaciniai technologiniai ištekliai;

3.2. kitos Veiklos tęstinumo valdymo plane vartojamos sąvokos atitinka Veiklos tęstinumo valdymo plano 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Veiklos tęstinumo valdymo plano tikslas – užtikrinti VLK valdomų informacinių sistemų ir ryšių technologijų (toliau – IRT) veiklos tęstinumą elektroninės informacijos saugos incidento metu, kilus pavojui informacinių sistemų duomenims, techninės ir programinės įrangos funkcionavimui. Veiklos tęstinumo valdymo planas skirtas spręsti saugos incidentams, dėl kurių gali atsirasti neteisėto prisijungimo prie informacinių sistemų ar ryšių technologijų galimybė, būti sutrikdyta ar pakeista IRT veikla, sunaikinta, sugadinta ar pakeista informacinių sistemų elektroninė informacija, panaikinta ar apribota galimybė naudotis informacinių sistemų elektronine informacija, sudarytos sąlygos neteisėtai pasisavinti elektroninę informaciją, ją paskleisti ar kitaip panaudoti.

5. Veiklos tęstinumo valdymo planu privalo vadovautis informacinių sistemų valdytojas, informacinių sistemų tvarkytojai, šių sistemų naudotojai ir saugos įgaliotiniai (-is) bei TLK saugos įgaliotiniai (toliau visi kartu – saugos įgaliotiniai), taip pat informacinių sistemų ir infrastruktūros administratoriai bei VLK kibernetinio saugumo vadovas.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

6. Veiklos tęstinumo valdymo planas taikomas IRT, jeigu nėra parengtų ir patvirtintų atskirų IRT veiklos tęstinumo valdymo planų.

7. Informacinių sistemų naudotojų, saugos įgaliotinių ir administratorių įgaliojimai bei atsakomybė yra nurodyti VLK valdomų informacinių sistemų naudotojų administravimo taisyklėse.

8. Informacinių sistemų naudotojai, pastebėję IRT veiklos sutrikimus, neveikiančias ar netinkamai veikiančias informacinių sistemų saugos užtikrinimo priemones, turi nedelsdami registruoti saugos incidentą Naudotojų pagalbos tarnybos informacinėje sistemoje (toliau – NAT IS), jei nėra galimybės registruoti – nedelsiant kitomis priemonėmis apie jį pranešti atsakingam (-iems) saugos įgaliotiniui (-iams), informacinių sistemų administratoriams ar VLK kibernetinio saugumo vadovui.

9. Informacinių sistemų naudotojai, sužinoję apie saugos incidentą, turi nedelsdami nutraukti darbą su IRT, jeigu tai yra būtina.

10. Saugos įgaliotinių, informacinių sistemų ir infrastruktūros administratorių, VLK kibernetinio saugumo vadovo ir kitų atsakingų darbuotojų atliekami veiksmai įvykus saugos incidentui yra nurodyti VLK valdomų IRT veiklos tęstinumo valdymo detaliajame plane (1 priedas).

11. IRT informacijos saugos incidento metu patirti nuostoliai padengiami iš VLK ir (ar) TLK biudžeto lėšų (veiklos išlaidų).

12. IRT veikla yra laikoma atkurta, jeigu ji atitinka šiuos veiklos kriterijus:

12.1. informacinių sistemų teikiami duomenys yra atnaujinami ir išsaugomi;

12.2. veikia atitinkamų informacinių sistemų integracinės duomenų mainų sąsajos, keičiamasi duomenimis su informacinių sistemų duomenų teikėjais / gavėjais;

12.3. IRT tampa prieinamos, tinkamai veikia jų funkcijos;

12.4. informacinių sistemų naudotojai gali atlikti savo darbo funkcijas informacinėse sistemose įprastu būdu.

13. Pagal Veiklos tęstinumo valdymo planą IRT neveikimo laikotarpis negali būti ilgesnis nei:

13.1. I kategorijos informacinių sistemų – 8 valandos;

13.2. II kategorijos informacinių sistemų – 12 valandų;

13.3. III kategorijos informacinių sistemų – 16 valandų;

13.4. IV kategorijos informacinių sistemų – 24 valandos.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

14. Elektroninės informacijos saugos ir kibernetiniams incidentams valdyti bei IRT veiklos atkūrimui organizuoti VLK direktoriaus įsakymu sudaromos ir tvirtinamos dvi grupės: Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė.

15. Veiklos tęstinumo valdymo grupę sudaro:

15.1. VLK Informacinių technologijų departamento (toliau – ITD) direktorius (darbo grupės pirmininkas);

15.2. VLK ITD Informacinių sistemų plėtros skyriaus vedėjas (darbo grupės pirmininko pavaduotojas);

15.3. VLK ITD Draudžiamųjų privalomuoju sveikatos draudimu registro skyriaus vedėjas;

15.4. informacinių sistemų saugos įgaliotiniai ir TLK saugos įgaliotiniai (jei būtina);

15.5. VLK kibernetinio saugumo vadovas;

15.6. *Neteko galios nuo 2021-04-01*

Papunkčio naikinimas:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

15.7. kiti informacinių sistemų valdytojo deleguoti ir VLK direktoriaus įsakymu paskirti valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis (jei būtina).

16. Veiklos tęstinumo valdymo grupės pagrindinis uždavinys – užtikrinti IRT veiklos tęstinumui kylančių grėsmių valdymą ir IRT veiklos atkūrimo koordinavimą, įvykus saugos incidentui.

17. Veiklos tęstinumo valdymo grupės funkcijos:

17.1. situacijos analizė ir sprendimų IRT veiklos tęstinumo valdymo klausimais priėmimas;

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

17.3. bendravimas su kitų susijusių organizacijų veiklos tęstinumo valdymo grupėmis;

17.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

17.5. finansinių ir kitų išteklių, būtinų veiklai atkurti įvykus saugos incidentui, naudojimo kontrolė;

17.6. elektroninės informacijos fizinės saugos užtikrinimas įvykus saugos incidentui;

17.7. logistika (žmonių, daiktų, įrangos gabenimas ir šio darbo organizavimas);

17.8. IRT veiklos atkūrimo priežiūra ir koordinavimas;

17.9. kitos Veiklos tęstinumo valdymo grupei pavestos funkcijos.

18. Veiklos atkūrimo grupę sudaro:

18.1. VLK ITD Informacinių sistemų priežiūros skyriaus vedėjas (darbo grupės pirmininkas);

Papunkčio pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

18.2. VLK ITD Informacinių sistemų priežiūros skyriaus vyriausiasis specialistas (darbo grupės pirmininko pavaduotojas);

Papunkčio pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

18.3. informacinių sistemų ir infrastruktūros administratoriai;

18.4. fizinės saugos įgaliotiniai (jei būtina);

18.5. kiti informacinių sistemų valdytojo deleguoti ir VLK direktoriaus įsakymu paskirti valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis (jei būtina);

19. Veiklos atkūrimo grupės pagrindinis uždavinys – vykdyti IRT atkūrimo darbus ir Veiklos tęstinumo valdymo grupės nurodymus, susijusius su informacinių sistemų funkcinių galimybių atkūrimu.

20. IRT veiklos atkūrimo grupės funkcijos:

20.1. tarnybinių stočių veiklos atkūrimo organizavimas;

20.2. kompiuterių tinklo veiklos atkūrimo organizavimas;

20.3. informacinių sistemų duomenų ir elektroninės informacijos atkūrimo organizavimas;

20.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

20.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

20.6. kitos IRT veiklos atkūrimo grupei pavestos funkcijos.

21. VLK valdomų IRT veiklos tęstinumo valdymo detaliajame plane nurodomas veiksmų eiliškumas, atsakingi vykdytojai, atskiri IRT veiklos atkūrimo, įvykus skirtingo pobūdžio ir masto elektroninės informacijos saugos incidentams, scenarijai.

22. Veiklos tęstinumo valdymo grupė ir veiklos atkūrimo grupė tarpusavyje ir su kitomis grupėmis bendrauja naudodamosi elektroniniu paštu, mobiliuoju ryšiu ir kitomis ryšio priemonėmis. Bendravimo dažnumą, įvertinusi saugos incidento mastą, pobūdį ir veiklos atkūrimo eigą, nustato Veiklos tęstinumo valdymo grupė pirmojo susitikimo metu. Bendraujama tol, kol bus pašalinti saugos incidento padariniai.

23. Veiklos tęstinumo valdymo grupės posėdį elektroninio ryšio priemonėmis organizuoja Veiklos tęstinumo valdymo grupės pirmininkas arba jo pavedimu – šios grupės narys.

24. Veiklos atkūrimo grupės posėdį elektroninio ryšio priemonėmis organizuoja veiklos atkūrimo grupės pirmininkas arba jo pavaduotojas. Saugos įgaliotiniai, administratoriai, įvertinę saugos kibernetinio incidento reikšmingumą, turi teisę inicijuoti Veiklos atkūrimo grupės posėdį būtiniems informacinių sistemų ar infrastruktūros veiklos atkūrimo veiksmams aptarti, suderinti arba organizuoti.

25. Įvykus saugos incidentui:

25.1. informacinių sistemų naudotojai privalo nedelsdami pranešti apie saugos incidentą, kaip numatyta Veiklos tęstinumo valdymo plano 8 punkte;

25.2. saugos incidentas aprašomas, nurodant jo vietą, laiką, pobūdį bei kitą su juo susijusią informaciją, ir registruojamas NAT IS;

25.3. saugos įgaliotiniai ar administratoriai, gavę pranešimą apie saugos incidentą, nedelsdami turi imtis reikiamų veiksmų saugos incidentui sustabdyti ir pranešti apie tai Veiklos tęstinumo valdymo grupės pirmininkui bei VLK kibernetinio saugumo vadovui;

25.4. informacinės sistemos saugos įgaliotinis (-iai) kartu su Veiklos atkūrimo grupe rengia ir koreguoja VLK valdomų IRT veiklos tęstinumo valdymo detalųjį planą ir teikia Veiklos tęstinumo valdymo grupei derinti;

25.5. VLK kibernetinio saugumo vadovas nustato saugos kibernetinio incidentų valdymo, tyrimo, šalinimo prioritetus ir apie juos informuoja Nacionalinį kibernetinio saugumo centrą VLK ir TLK organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo, patvirtinto VLK direktoriaus 2017 m. kovo 9 d. įsakymu Nr. 1K-52 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo patvirtinimo“, nustatyta tvarka;

25.6. Veiklos atkūrimo grupės nariai pagal kompetenciją atkuria informacinių sistemų tarnybinės stoties bei programinės įrangos veikimą ir apie atliktus veiksmus nedelsdami informuoja informacinės sistemos saugos įgaliotinį (-ius) bei Veiklos tęstinumo valdymo grupės pirmininką;

25.7. Veiklos tęstinumo valdymo grupės vadovas organizuoja žalos informacinių sistemų elektroninei informacijai, informacinių sistemų techninei bei programinei įrangai vertinimą,

koordinuoja techninės, sisteminės ir taikomosios programinės įrangos, būtinos informacinės sistemos veiklai atkurti, įsigijimą.

26. Techninė, sisteminė ir taikomoji programinė įranga, kuria turi būti pakeista saugos incidento metu sunaikinta ar sugadinta įranga, įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo ir (ar) VLK direktoriaus įsakymu tvirtinamų supaprastintų viešųjų pirkimų taisyklių nustatyta tvarka.

27. Nesant galimybių tęsti veiklą pagrindinėse informacinių sistemų patalpose, šių sistemų įranga gali būti per 1 darbo dieną laikinai perkeliama į atsargines patalpas, tenkinančias minimalius pagrindinėms patalpoms keliamus reikalavimus, numatytus VLK ir TLK fizinės saugos tvarkos apraše, patvirtintame VLK direktoriaus 2018 m. sausio 11 d. įsakymu Nr.1K-9 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų fizinės saugos tvarkos aprašo patvirtinimo“. Atsarginėms patalpoms taikomi šie reikalavimai:

27.1. šios patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

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

27.3. šios patalpos turi būti apsaugotos skirtingos konstrukcijos spynomis;

27.4. šiose patalpose turi būti įrengtas rezervinis elektros energijos šaltinis, užtikrinantis įrangos veikimą ne trumpiau kaip 30 minučių;

27.5. šiose patalpose nuolat turi veikti oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema).

28. Įvykus saugos incidentui, dėl kurio negalima atkurti IRT veiklos VLK patalpose, ši veikla atkuriama vienoje iš TLK: Vilniaus TLK (Ž. Liauksmino g. 6, LT-01101 Vilnius), Kauno TLK (Aukštaičių g. 10, LT-44147 Kaunas), Klaipėdos TLK (Pievų Tako g. 38, LT-92236 Klaipėda), Šiaulių TLK (Vilniaus g. 273, LT-76332 Šiauliai), Panevėžio TLK (Respublikos g. 66, LT-35158 Panevėžys).

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

29. Informacija apie informacinių sistemų techninę ir programinę įrangą (šios įrangos parametrus) pateikiama kiekvienos iš šių sistemų techniniame apraše (specifikacijoje) ir detalaus projektavimo dokumente. Už šios įrangos priežiūrą yra atsakingi administratoriai.

30. Minimalaus funkcionalumo informacinių technologijų įrangos (šios įrangos parametrų), reikiamos IRT veiklai užtikrinti saugos incidento metu, specifikacija atitinka pagrindinę jų techninės ir programinės įrangos specifikaciją.

31. VLK pastato, kuriame yra informacinių sistemų ir infrastruktūros įranga, patalpų brėžiniai (juose pažymėtos tarnybinės stotys, kompiuterių tinklo ir telefonų tinklo mazgai, kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos, taip pat elektros įvedimo pastate vietos) rengiami, atnaujinami ir saugomi VLK Bendrųjų reikalų skyriuje.

32. Kompiuterinės ir techninės įrangos priežiūros sutartis, kompiuterių tinklo fizinio ir loginio sujungimo schemas, taip pat programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo duomenis rengia, atnaujina ir saugo VLK ITD Informacinių sistemų priežiūros skyriaus atsakingieji darbuotojai.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

33. Programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta bei šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos nurodytos Elektroniniu būdu tvarkomų duomenų atsarginių kopijų valdymo tvarkos apraše, patvirtintame VLK direktoriaus 2020 m. gruodžio 23 d. įsakymu Nr. 1K- 386 „Dėl Elektroninių duomenų kopijų darymo tvarkos aprašo patvirtinimo“.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

34. Elektroninės informacijos teikimo ir kompiuterinės, techninės bei programinės įrangos, jos priežiūros sutartys saugomos Dokumentų valdymo informacinėje sistemoje. Kiekvienoje sutartyje yra nurodytos asmenų, atsakingų už šių sutarčių įgyvendinimo priežiūrą, pareigos ir kontaktinė informacija.

35. Jeigu VLK ar TLK naudoja (pagal nuomos, panaudos ar kitas sutartis) visą informacinės sistemos techninę įrangą ar jos dalį, priklausančias trečiajai šaliai ir esančias jos patalpose, sutarties su trečiąja šalimi data, numeris ir sutarties kopija saugoma Dokumentų valdymo informacinėje sistemoje.

36. Jeigu IRT veiklos atkūrimo atžvilgiu susidaro ekstremali padėtis, kai atitinkamos informacinės sistemos ar infrastruktūros administratorius negali dėl komandiruotės, ligos ar kitų priežasčių operatyviai atvykti į darbo vietą ir vietoj jo atvyksta jį pavaduojantis asmuo, šio asmens minimalus kompetencijos ar žinių lygis negali būti žemesnis už atitinkamos informacinės sistemos administratoriui keliamų reikalavimų lygį.

37. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašus su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis ne darbo metu, rengia ir atnaujina VLK ITD Informacinių sistemų priežiūros skyriaus ir Informacinių sistemų plėtros skyriaus atsakingieji darbuotojai.

Punkto pakeitimai:
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576

38. VLK darbuotojų sąrašas, kuriame nurodyti darbuotojų darbo telefonai, skelbiamas VLK interneto svetainėje www.vlk.lt, TLK darbuotojų – TLK interneto svetainėse.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

39. Veiklos tęstinumo valdymo plano veiksmingumas išbandomas ne rečiau kaip kartą per dvejus metus. Plano veiksmingumas nėra bandomas jeigu einamaisiais metais įvyko saugos incidentas, dėl kurio buvo vykdomas VLK valdomų informacinių sistemų ir ryšių technologijų veiklos tęstinumo valdymo detalusis planas.

40. Veiklos tęstinumo valdymo plano veiksmingumas išbandomas saugos incidento teorinio modeliavimo, simuliacinio žaidimo ar kitu būdu, kuriame turi būti imituojamas IRT veiklos sutrikimas. Plano veiksmingumo bandymo metu užpildoma VLK IRT veiklos atkūrimo (išbandymo) detaliojo plano forma (2 priedas).

41. Kibernetinių incidentų imitavimo (įsilaužimo testavimo) pratybos turi būti organizuojamos kartą per metus. Imituojamo incidento metu už saugos kibernetinio incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus; iš atsarginių informacinių sistemų duomenų kopijų atkuriami duomenys ir elektroninė informacija.

42. Jeigu Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu nustatoma incidentų valdymo ir šalinimo, taip pat VLK nepertraukiamos veiklos užtikrinimo trūkumų, šis planas yra tikslinamas.

43. Pastebėtų trūkumų šalinimo prioritetai, reikiamos lėšos šiems trūkumams pašalinti, laikotarpis, per kurį trūkumai turi būti pašalinti, ir atsakingi už trūkumų pašalinimą asmenys nustatomi bendrame Veiklos atkūrimo grupės ir Veiklos tęstinumo valdymo grupės posėdyje.

44. Pagal bandymų rezultatus parengiama Veiklos tęstinumo valdymo plano veiksmingumo išbandymo įvertinimo ataskaita (laisvos formos). Šioje ataskaitoje nurodoma išbandymo data, eiga ir aprašomi rezultatai. Veiklos atkūrimo grupės vadovas ir informacijos saugos įgaliotiniai yra

atsakingi už Veiklos tęstinumo valdymo plano veiksmingumo išbandymo įvertinimo ataskaitos parengimą. Ataskaitą tvirtina VLK Informacinių technologijų departamento direktorius.

45. Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami laikantis šių principų:

45.1. operatyvumo – kiek galima greičiau pašalinti trūkumus. Atliekant trūkumų šalinimo veiklą, turi būti atsižvelgiama į trūkumų sudėtingumą ir apimtį. Saugos įgaliotiniai nusprendžia ir nustato, per kiek laiko turi būti atliktas konkretus trūkumų šalinimo veiksmas ir pašalinti trūkumai;

45.2. veiksmingumo – trūkumų šalinimas laikomas veiksmingu, jei pavyksta sumažinti konkretaus trūkumo daromą neigiamą poveikį informacinėms sistemoms;

45.3. ekonomiškumo – pašalinti visus trūkumus taupiai naudojant turimus išteklius.

_____

Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų ir ryšių technologijų veiklos tęstinumo valdymo plano
1 priedas

VLK VALDOMŲ INFORMACINIŲ SISTEMŲ IR RYŠIŲ TECHNOLOGIJŲ VEIKLOS TĘSTINUMO VALDYMO DETALUSIS PLANAS

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
1. Nepasiekiamos patalpos (vykdoma evakuacija dėl gaisro, patalpų užpuolimo, pavojingų medžiagų patalpose, patalpų pažeidimo arba praradimo, stichinės nelaimės, oro sąlygų, avarijų, karo veiksmų)	1.1. Evakuojami darbuotojai ir atliekami kiti veiksmai pagal civilinės saugos planą, priešgaisrinę instrukciją ir pan.	Fizinės saugos įgaliotinis arba direktoriaus įsakymu paskirtas atsakingas asmuo	Nedelsiant
	1.2. Įvertinama, ar kyla pavojus nepertraukiamai VLK informacinių sistemų veiklai. Jei ne, toliau atliekami veiksmai, numatyti 1.9 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 1.3 papunktyje.	Veiklos tęstinumo valdymo grupė	Per 30 min. po incidento nustatymo
	1.3. Įvertinama, ar reikia išjungti informacines sistemas. Jei ne, toliau atliekami veiksmai, numatyti 1.5 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 1.4 papunktyje.	Veiklos tęstinumo valdymo grupė, Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo
	1.4. Jei reikia, išjungiamos informacinės sistemos (gali būti vykdoma nuotoliniu būdu)	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo
	1.5 Nustatoma, ar pasiekiama serverinė. Jei ne, toliau atliekami veiksmai, numatyti 1.6 papunktyje.	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	Jei taip, toliau atliekami veiksmai, numatyti 1.7 papunktyje.		
	1.6. Atliekami veiksmai, numatyti 2 incidentui šalinti.	Veiklos atkūrimo grupė	Terminai numatyti 2 incidento šalinimo scenarijuje
	1.7. Priimamas sprendimas, ar reikia atkurti informacinių sistemų veiklą. Jei ne, toliau atliekami veiksmai, numatyti 1.9 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 1.8 papunktyje.	Veiklos tęstinumo valdymo grupė	Per dvi darbo valandas po incidento nustatymo
	1.8. Atkuriama informacinių sistemų veikla.	Veiklos atkūrimo grupė	Per tris darbo dienas po incidento nustatymo
	1.9. Įvertinama, ar reikia imtis papildomų priemonių. Jei ne, laikoma, kad informacinių sistemų veikla atkurta. Jei taip, toliau atliekami veiksmai, numatyti 1.10 papunktyje.	Veiklos tęstinumo valdymo grupė	Per dvi darbo valandas po incidento nustatymo
	1.10. Taikomos papildomos priemonės.	Veiklos atkūrimo grupė	Per penkias darbo dienas po incidento nustatymo
	1.11 Informuojami darbuotojai apie patalpų pasiekiamumą, kai gaunama informacija, kad patalpos tinkamos naudoti.	Fizinės saugos įgaliotinis arba direktoriaus įsakymu paskirtas atsakingas asmuo	Per vieną darbo valandą po incidento pašalinimo
2. Nepasiekiama serverinė (dėl	2.1. Nustatoma, kad serverinė yra nepasiekiama.	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
gaisro pastato dalyje, kurioje yra duomenų centras, dėl inžinerinių sistemų gedimo (rezervinės elektros maitinimo, kondicionavimo ir vėdinimo ar pan.)	2.2. Įvertinama, ar reikia atkurti informacinių sistemų veiklą atsarginėse patalpose. Jei ne, toliau atliekami veiksmai, numatyti 2.4 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 2.3 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	2.3. Atkuriamos informacinės sistemos atsarginėse patalpose. Toliau atliekami veiksmai, numatyti 2.4 papunktyje.	Veiklos atkūrimo grupė	Per penkias darbo dienas po incidento nustatymo
	2.4. Įvertinama, ar reikia imtis papildomų priemonių. Jei ne, toliau atliekami veiksmai, numatyti 2.6 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 2.5 papunktyje.	Veiklos tęstinumo valdymo grupė	Per dvi darbo valandas po informacinių sistemų veiklos atkūrimo atsarginėse patalpose
	2.5. Taikomos papildomos priemonės. Toliau atliekami veiksmai, numatyti 2.4 papunktyje.	Veiklos atkūrimo grupė	Per dvi darbo dienas po informacinių sistemų veiklos atkūrimo atsarginėse patalpose
	2.6. Įvertinama, ar galima grįžti į serverinę. Jei ne, toliau atliekami veiksmai, numatyti 2.4 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 2.7 papunktyje.	Veiklos tęstinumo valdymo grupė Veiklos atkūrimo grupė	Per dvi darbo valandas po informacinių sistemų serverinės veiklos atkūrimo
	2.7. Atkuriamos informacinės sistemos serverinėje. Informacinių sistemų veikla atkurta.	Veiklos atkūrimo grupė	Per penkiolika valandų po incidento nustatymo
3. Nepasiekiama techninė įranga (dėl techninės įrangos gedimo, kai	3.1. Nustatoma, kad nepasiekiama techninė įranga.	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo
	3.2. Įvertinama situacija, jei reikia, informuojamos draudimo įmonės, kitos institucijos.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
nėra rezervinės įrangos ir nepavyksta atkurti informacinių sistemų veiklos per 1 val. po įvykio, be to, manoma, kad nepavyks atkurti šių sistemų veiklos pagal teisės aktų nustatytus terminus)	3.3 Nustatoma, ar yra pakankamai išteklių (techninių) funkcijoms perkelti. Jei ne, toliau atliekami veiksmai, numatyti 3.5 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 3.4 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	3.4. Funkcijos perkeliamos pasinaudojant laisvais ištekliais. Toliau vykdomi veiksmai, numatyti 3.5 papunktyje.	Veiklos atkūrimo grupė	Per penkiolika valandų po incidento nustatymo
	3.5. Nustatoma, ar pasiekiama serverinė. Jei ne, toliau atliekami veiksmai, numatyti 2 incidentui šalinti. Jei taip, toliau atliekami veiksmai, numatyti 3.6 papunktyje.	Veiklos tęstinumo valdymo grupė	Jei ne, terminai numatyti pagal 2 incidento scenarijų. Jei taip, per 30 min. po incidento nustatymo
	3.6. Nustatoma, ar reikia įsigyti papildomų išteklių. Jei ne, toliau atliekami veiksmai, numatyti 3.8 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 3.7 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą
	3.7. Įsigyjami papildomi ištekliai.	Veiklos tęstinumo valdymo grupė, Veiklos atkūrimo grupė	Per penkias darbo dienas
	3.8. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau atliekami veiksmai, numatyti 3.10 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 3.9 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo dieną po papildomų išteklių įsigijimo

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	3.9. Taikomos papildomos priemonės. Toliau atliekami veiksmai, numatyti 3.8 papunktyje.	Veiklos atkūrimo grupė	Per vieną darbo dieną po papildomų išteklių įsigijimo
	3.10. Priimamas sprendimas, kad funkcijos yra atkurtos.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po funkcijų atkūrimo
4. Nepasiekiami ar sugadinti duomenys (kai yra pažeistas duomenų bazės integralumas, sugadinti duomenys atsarginėse kopijose, dėl kenksmingos programinės įrangos, dėl elektromagnetinio poveikio)	4.1. Nustatoma, kad duomenys yra nepasiekiami.	Veiklos atkūrimo grupė	Per vieną darbo valandą po incidento nustatymo
	4.2. Įvertinama, ar reikia atkurti techninę įrangą. Jei ne, toliau atliekami veiksmai, numatyti 4.3 papunktyje. Jei taip, toliau atliekami veiksmai pagal 3 incidento šalinimo scenarijų.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	4.3. Nustatoma, ar yra duomenų atsarginės kopijos. Jei ne, toliau atliekami veiksmai, numatyti 4.5 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 4.4 papunktyje.	Veiklos atkūrimo grupė, Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	4.4. Atkuriami duomenys iš atsarginių kopijų.	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo
	4.5. Nustatoma, ar reikia įvesti duomenis. Jei ne, toliau atliekami veiksmai, numatyti 4.7 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 4.6 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	4.6. Duomenys įvedami rankiniu būdu arba importuojami iš kitų šaltinių.	Veiklos atkūrimo grupė	Per penkiolika valandų

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	4.7. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau atliekami veiksmai, numatyti 4.9 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 4.8 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	4.8. Taikomos papildomos priemonės.	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo
	4.9. Duomenys yra pasiekiami.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po duomenų atkūrimo
5. Nepasiekiami ryšiai (dėl kibernetinių atakų, dėl dingusio ryšio su paslaugų teikėju (interneto), optinių kabelių nutrūkimo, kai neveikia sąsajos su išorinėmis sistemomis)	5.1 Nustatoma, kad ryšiai yra nepasiekiami.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą
	5.2. Atliekama situacijos analizė ir naudotojai informuojami apie sutrikimus.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	5.3. Nustatoma, ar reikia organizuoti alternatyvius ryšius. Jei ne, toliau atliekami veiksmai, numatyti 5.5 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 5.4 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	5.4. Organizuojamos alternatyvios ryšio priemonės.	Veiklos atkūrimo grupė	Per penkiolika valandų po incidento nustatymo
	5.5. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau atliekami veiksmai, numatyti 5.7 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 5.6 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
	5.6. Taikomos papildomos priemonės.	Veiklos atkūrimo grupė	Per vieną darbo dieną po incidento nustatymo

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	5.7. Ryšiai yra atkurti.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po incidento nustatymo
6. Nepasiekiami darbuotojai (kai negali atvykti į darbą daugiau nei penktadalis darbuotojų dėl oro sąlygų, stichinių nelaimių, avarijų, epidemijų, mobilizacijos, cheminės atakos, karo veiksmų ir pan.)	6.1. Nustatoma, kad darbuotojai yra nepasiekiami.	Veiklos tęstinumo valdymo grupė	Per vieną darbo dieną po incidento nustatymo
	6.2. Atliekama situacijos analizė.	Veiklos tęstinumo valdymo grupė	Per vieną darbo dieną po incidento nustatymo
	6.3. Nustatoma, ar reikia samdyti išorinius paslaugų teikėjus. Jei ne, toliau atliekami veiksmai, numatyti 6.5 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 6.4 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po situacijos analizės
	6.4. Samdomi išoriniai paslaugų teikėjai.	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	6.5. Nustatoma, ar reikia samdyti papildomus darbuotojus. Jei ne, toliau atliekami veiksmai, numatyti 6.7 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 6.6 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po situacijos analizės
	6.6. Samdomi papildomi darbuotojai.	Veiklos atkūrimo grupė	Per teisės aktuose numatytą terminą
	6.7. Nustatoma, ar reikia imtis papildomų priemonių. Jei ne, toliau atliekami veiksmai, numatyti 6.9 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 6.8 papunktyje.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą
	6.8. Taikomos papildomos priemonės.	Veiklos atkūrimo grupė	Per vieną darbo dieną

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	6.9. Laikoma, kad funkcijos yra atkurtos	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą

_____

Valstybinės ligonių kasos prie Sveikatos apsaugos
ministerijos valdomų informacinių ir ryšių technologijų veiklos
tęstinumo valdymo plano
2 priedas

(Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos informacinių sistemų ir ryšių technologijų veiklos atkūrimo (išbandymo) detaliojo plano forma)

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINIŲ SISTEMŲ IR RYŠIŲ TECHNOLOGIJŲ VEIKLOS ATKŪRIMO (IŠBANDYMO) DETALUSIS PLANAS

Elektroninės informacijos saugos ar kibernetinio saugumo incidento Nr.

Eil. Nr.	Elektroninės informacijos ar kibernetinės saugos incidento pavadinimas	Atliekami veiklos atkūrimo veiksmai	Atsakingas vykdytojas	Įgyvendinimo data	Rezultatas / pastabos

Parengė	_____
	(Pareigos, vardas pavardė, parašas, data)

Pakeitimai:

1.
Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. 1K-109, 2021-03-31, paskelbta TAR 2021-03-31, i. k. 2021-06576
Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2020 m. vasario 14 d. įsakymo Nr. 1K-45 „Dėl Valstybinės ligonių kasos prie sveikatos apsaugos ministerijos valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“ pakeitimo