Suvestinė redakcija nuo 2023-09-26

Įsakymas paskelbtas: TAR 2021-03-08, i. k. 2021-04706

**VALSTYBINĖS LIGONIŲ KASOS
PRIE SVEIKATOS APSAUGOS MINISTERIJOS
DIREKTORIUS**

ĮSAKYMAS
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

2020 m. vasario 14 d. Nr. 1K-45
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7 ir 8 punktais:

1. T v i r t i n u:

1.1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles (pridedama).

1.2. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų naudotojų administravimo taisykles (pridedama).

1.3. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų ir ryšių technologijų veiklos tęstinumo valdymo planą (pridedama).

2. P a v e d u šio įsakymo vykdymą kontroliuoti Informacinių technologijų departamento direktoriui.

Direktorius Gintaras Kacevičius

SUDERINTA
Nacionalinio kibernetinio saugumo centro

prie Krašto apsaugos ministerijos
2020 m. vasario 11 d. raštu Nr. (4.1 E) 6K-101

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 SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią saugų Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) ir teritorinių ligonių kasų (toliau – TLK) (VLK ir TLK kartu toliau – ligonių kasos) informacinių sistemų, išvardytų VLK valdomų informacinių sistemų duomenų saugos nuostatų, patvirtintų 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 punkte, Detalios paciento lygio sąnaudų apskaitos informacinės sistemos bei vidaus administravimui skirtų informacinių sistemų tvarkymą ir šių informacinių sistemų kibernetinio saugumo politikos įgyvendinimą.

2. Taisyklės parengtos vadovaujantis:

2.1. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

2.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.3. 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“;

2.4. 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“.

2.5. Duomenų saugos nuostatais,

2.6. VLK ir TLK organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu, patvirtintu 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“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

2.7. kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

2.8. LST ISO/IEC 27001 (aktualios redakcijos) „Informacijos saugumo valdymo sistemos. Reikalavimai“.

3. Taisyklėse vartojamos sąvokos:

3.1. **VLK informacinės sistemos naudotojas** – ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, bei išorės naudotojai, turintys teisę naudotis VLK informacinių sistemų ištekliais tam tikroms funkcijoms atlikti.

3.2. **Informacinių sistemų administratoriai** – ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, arba trečiųjų šalių darbuotojai pagal sutartį teikiantys priežiūros, diegimo ar kitas paslaugas, susijusias su informacinėmis technologijomis, ir turintys teisę naudotis VLK informacinių sistemų ištekliais tam tikroms funkcijoms atlikti.

3.3. Kitos sąvokos, atitinkančios Taisyklių 2 punkte nurodytuose teisės aktuose vartojamas sąvokas.

4. Ligonių kasos, užtikrindamos elektroninės informacijos saugą, vadovaujasi Lietuvos standartais LST ISO/IEC 27002 (aktualios redakcijos) „Informacijos saugumo valdymo praktikos kodeksas“, LST ISO/IEC 27001 (aktualios redakcijos) „Informacijos saugumo valdymo sistemos. Reikalavimai “, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą.

5. VLK informacinėse sistemose tvarkoma elektroninė informacija yra nurodyta šių sistemų nuostatuose.

6. VLK informacinėse sistemose tvarkoma skirtingos svarbos elektroninė informacija. Atitinkamos VLK informacinės sistemos svarbos kategorija ir priskyrimo šiai kategorijai kriterijai nurodyti Duomenų saugos nuostatų 19–22 punktuose.

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

7. Už VLK informacinių sistemų elektroninės informacijos saugų tvarkymą atsako atitinkamų VLK informacinių sistemų naudotojai pagal jiems suteiktas informacinių sistemų duomenų tvarkymo teises.

8. VLK informacinių sistemų administratoriai atsako už atitinkamų informacinių sistemų taikomosios programinės įrangos ir duomenų bazės administravimą, prieigų prie informacinių sistemų suteikimą naudotojams, šių prieigų pakeitimą ar panaikinimą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

9. Informacinių sistemų kompiuterinės įrangos saugos priemonės:

9.1. kompiuterinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų ir užtikrinamas šios įrangos gamintojų garantinis aptarnavimas;

9.2. visose tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti įdiegta ir reguliariai atnaujinama virusų bei kitų kenkėjų kodo aptikimo ir šalinimo antivirusinė programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti. Kompiuterizuotose darbo vietose turi būti naudojamos ir reguliariai atnaujinamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės;

9.3. tarnybinės stotys turi būti apsaugotos nuo elektros srovės svyravimų ir (ar) nutrūkimo naudojant rezervinius elektros įvadus, vietinį elektros generatorių, nenutrūkstamo svarbiausios kompiuterinės įrangos maitinimo šaltinius (UPS), užtikrinančius šios įrangos veikimą ne mažiau kaip 60 min.;

9.4. tarnybinėse stotyse ir kompiuterizuotuose darbo vietose turi būti įdiegtos darbo parametrų stebėjimo ir valdymo funkcijos; turi būti siunčiami perspėjimai, kai pagrindinėje kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, arba ilgą laiką labai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

9.5. pagrindinės tarnybinės stotys, svarbiausi duomenų perdavimo tinklo mazgai ir ryšio linijos esant techninių galimybių turi būti dubliuojami ir jų techninė būklė nuolat stebima;

9.6. svarbiausios kompiuterinės įrangos gedimai turi būti registruojami atsakingų administratorių;

9.7. naudotojų kompiuteriai turi būti tinkamai paruošti darbui nustatyta tvarka, turi būti įdiegti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

9.8. nuotolinis prisijungimas prie kompiuterinės įrangos turi būti vykdomas algoritmu (protokolu), skirtu duomenims šifruoti (SSL/TLS/VPN/SSH);

9.9. tiesioginė prieiga prie tarnybinių stočių suteikiama tik informacinių sistemų administratoriams;

9.10. kitos kompiuterinės įrangos saugos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

10. Ligonių kasų informacinių sistemų sisteminės ir taikomosios programinės įrangos saugos priemonės:

10.1. VLK informacinių sistemų programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

10.2. kompiuterizuotose darbo vietose darbo funkcijoms vykdyti turi būti naudojama tik legali, patikrinta, patikimų gamintojų programinė įranga, naudojama darbo funkcijoms vykdyti įtraukta į leistinos programinės įrangos sąrašą;

10.3. programinės įrangos testavimas turi būti atliekamas naudojant atitinkamą testavimo aplinką;

10.4. programinės įrangos diegimą, konfigūravimą ir šalinimą turi vykdyti atitinkamos informacinės sistemos administratorius arba šių paslaugų teikėjų atsakingas darbuotojas pagal atitinkamų paslaugų teikimo ir priežiūros sutartį;

10.5. programinės įrangos gedimai turi būti registruojami VLK naudotojų aptarnavimo tarnybos informacinėje sistemoje;

10.6. VLK informacinių sistemų naudotojams nesinaudojant kompiuterių įranga ilgiau nei 15 minučių, kompiuteriai turi būti užrakinami automatiškai, iš naujo prie jų prisijungti turi būti galima tik pakartotinai patvirtinus savo tapatybę;

10.7. kitos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

11. VLK informacinių sistemų elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1. informacinių sistemų 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 pagal naujausias gamintojo rekomendacijas;

11.2. informacinės sistemos programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų – SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*) ir kitų;

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

11.4. nuotoliniu būdu prisijungiantys VLK informacinių sistemų naudotojai, kurie duomenis perduoda ir gauna viešaisiais telekomunikacijų tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą arba virtualų privatų tinklą;

11.5. kitos priemonės yra numatytos Kibernetinio saugumo reikalavimų aprašo priede.

12. Tarnybinių stočių patalpų ir aplinkos saugumo užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga):

12.1. patalpose turi būti įrengtos nedegios metalinės, atsparios laužimui, savaime užsidarančios ir visada rakinamos durys;

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

12.3. patalpose turi būti įrengtas šildymas, vėdinimas ir oro kondicionavimas (turi būti priežiūros sutartys);

12.4. patalpose turi būti įrengta įsilaužimo signalizacija (garsinė, judesio);

12.5. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

12.6. patekimas į patalpas, kuriose yra tarnybinės stotys, ir patalpas, kuriose saugomos atsarginės kopijos, kontroliuojamas naudojant vaizdo stebėjimo sistemą;

12.7. įėjimo į patalpas kontrolę vykdo VLK arba TLK fizinės saugos įgaliotinis;

12.8. į VLK tarnybinių stočių patalpas gali patekti tik VLK direktoriaus patvirtintame sąraše išvardyti darbuotojai. Į TLK tarnybinių stočių patalpas gali patekti tik TLK direktoriaus patvirtintame sąraše išvardyti darbuotojai. Įeinančių į patalpas asmenų tapatybė nustatoma ir fiksuojama elektroninės tapatybės nustatymo ir praėjimo kontrolės sistemoje (naudojama elektroninės tapatybės nustatymo kortelė). Jei elektroninės tapatybės nustatymo ir praėjimo kontrolės sistemos nėra, naudojami fiziniai raktai ir įėjimo žurnalai;

12.9. tarnybinių stočių valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į tarnybinių stočių patalpas;

12.10. kitos tarnybinių stočių patalpų ir aplinkos saugumo užtikrinimo priemonės numatytos VLK ir TLK fizinės saugos tvarkos apraše, kuris tvirtinamas VLK direktoriaus įsakymu.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

13. VLK informacinių sistemų duomenis įvesti, keisti ir atnaujinti gali tik šių informacinių sistemų naudotojai pagal jiems suteiktas prieigos teises.

14. VLK informacinių sistemų elektroninė informacija įrašoma, atnaujinama, keičiama ir naikinama vadovaujantis atitinkamos VLK informacinės sistemos nuostatais, Duomenų saugos nuostatais ir kitais teisės aktais, reglamentuojančiais informacinių sistemų elektroninės informacijos tvarkymą.

15. VLK informacinių sistemų naudotojų duomenis įvesti, keisti, atnaujinti gali tik informacinių sistemų administratoriai.

16. Duomenų bazėje tvarkomus duomenis įvesti, keisti, atnaujinti gali tik informacinės sistemos administratorius pagal jam suteiktas prieigos teises, gavęs konkrečią užduotį VLK naudotojų aptarnavimo informacinėje sistemoje arba Naudotojų tapatybių ir teisių valdymo sistemoje.

17. Informacinių sistemų naudotojų veiksmai turi būti registruojami toliau nurodytu būdu:

17.1. informacinių sistemų naudotojų tapatybė ir veiksmai, atliekami su informacinių sistemų duomenimis, fiksuojami programinėmis priemonėmis;

17.2. informacinių sistemų naudotojų veiksmai įrašomi automatiniu būdu ligonių kasų informacinių sistemų duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jo duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo. Šio žurnalo duomenys yra prieinami informacinių sistemų administratoriams pagal jų atliekamas darbo funkcijas.

18. Atsarginės VLK informacinių sistemų elektroninės informacijos (duomenų) kopijos daromos vadovaujantis Elektroniniu būdu tvarkomų duomenų atsarginių kopijų valdymo tvarkos aprašu, patvirtintu VLK direktoriaus įsakymu.

19. Prarasti, iškraipyti ar sunaikinti informacinių sistemų duomenys atkuriami iš atsarginių duomenų kopijų.

20. Duomenų atkūrimas iš atsarginių kopijų turi būti periodiškai išbandomas – ne rečiau kaip kartą per metus, išskyrus atvejus, kai duomenų atkūrimas vyksta realiu laiku.

21. Elektroninės informacijos mainai tarp ligonių kasų informacinių sistemų ir išorinių informacinių sistemų vykdomi duomenų teikimo sutartyse su šių informacinių sistemų valdytojais numatyta apimtimi, būdais ir terminais.

22. VLK informacinių sistemų elektroninė informacija kitiems registrams ir informacinėms sistemoms perduodama vadovaujantis atitinkamos informacinės sistemos nuostatais ir kitais saugų elektroninės informacijos tvarkymą reglamentuojančiais teisės aktais.

23. Už informacinių sistemų duomenų mainus ir gaunamos elektroninės informacijos atnaujinimą atsako informacinių sistemų administratoriai.

24. Informacinių sistemų administratoriai, užtikrindami informacinių sistemų elektroninės informacijos vientisumą, turi naudoti visas įmanomas technines, programines ir administracines priemones, skirtas informacinių sistemų elektroninei informacijai apsaugoti nuo neteisėtų veiksmų.

25. VLK informacinių sistemų naudotojai, pastebėję Duomenų saugos nuostatų, saugos politikos įgyvendinamųjų dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, turi registruoti Naudotojų aptarnavimo tarnybos informacinėje sistemoje incidentą arba pranešti apie tai atitinkamos informacinės sistemos saugos įgaliotiniui. Atsakingi darbuotojai, pasinaudoję atitinkamos duomenų bazės veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su VLK informacinės sistemos programine įranga ir duomenimis.

26. Jeigu atitinkamų informacinių sistemų naudotojai neinformuoja šių sistemų saugos įgaliotinių apie Taisyklių 25 punkte nurodytus pažeidimus, šių sistemų administratoriai juos informuoja apie tai elektroninėmis priemonėmis.

27. VLK informacinių sistemų kompiuterių, tarnybinių stočių techninę ir programinę įrangą diegia, keičia ir atnaujina atitinkamų informacinių sistemų administratoriai.

28. Planuodamas atitinkamos VLK informacinės sistemos techninės ir programinės įrangos keitimą, kurio metu galimi šios informacinės sistemos veikimo sutrikimai, jos administratorius privalo ne vėliau kaip prieš 4 valandas iki techninės ir programinės įrangos pakeitimo pradžios informuoti šios VLK informacinės sistemos naudotojus apie tokių darbų pradžią ir galimus sutrikimus.

29. Perduodant remontuoti sugedusią techninę įrangą, išimamos duomenų laikmenos (kietieji diskai ir kt.) arba daromos jų kopijos ir laikmenose saugomi duomenys ištrinami.

30. Atlikus programinės ir techninės įrangos keitimą, turi būti organizuojami atitinkamos VLK informacinės sistemos naudotojų darbo su nauja programine ir technine įranga mokymai. Mokomosios medžiagos garso ir vaizdo įrašai saugomi 3 metus po sistemos likvidavimo.

Punkto pakeitimai:
Nr. 1K-246, 2023-09-25, paskelbta TAR 2023-09-25, i. k. 2023-18632

31. VLK informacinių sistemų pokyčių valdymą planuoja ir užtikrina VLK informacinių sistemų valdytojas. Šis planavimas apima pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar techninis), įtakos vertinimą (svarbumas ir skubumas), pokyčių prioritetų nustatymą (eiliškumas).

32. VLK informacinių sistemų pokyčiai valdomi vadovaujantis Informacinių technologijų paslaugų gyvavimo ciklo valdymo tvarkos aprašo, patvirtinto VLK direktoriaus įsakymu, nuostatomis.

33. VLK informacinių sistemų pokyčiai numatomi pagal atitinkamų informacinių sistemų naudotojų ir administratorių poreikius, įvertinus techninės ir programinės įrangos naudojimo problemas, gerąją praktiką.

34. Jei įtariama grėsmė elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, prieš atliekant VLK informacinių sistemų pakeitimus jie turi būti išbandomi testavimo aplinkoje, identiškoje gamybinei aplinkai.

35. Sėkmingai išbandžius VLK informacinių sistemų pakeitimus testavimo aplinkoje, atitinkami pakeitimai atliekami gamybinėje aplinkoje.

36. VLK informacinių sistemų naudotojai (tik ligonių kasų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis) nešiojamuosius kompiuterius ir kitus mobiliuosius įrenginius naudoja tik tarnybinėms funkcijoms vykdyti.

37. Techninės įrangos (įskaitant stacionarius ir nešiojamuosius kompiuterius, mobiliuosius įrenginius ir kt.) naudojimo tvarką nustato VLK informacinių sistemų valdytojas, kuris turi numatyti:

37.1. techninės ir programinės įrangos apskaitos tvarkymą;

37.2. atitinkamus draudimus VLK informacinių sistemų naudotojams dirbant su technine ir programine įranga;

37.3. techninių įrenginių skyrimo ir naudojimo tvarką;

37.4. kenksmingos programinės įrangos aptikimo priemones; techninio aptarnavimo sąlygas ir pan.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

38. Reikalavimai paslaugoms, užtikrinančioms tinkamą VLK informacinių sistemų funkcionavimą, ir šių paslaugų teikėjams nustatomi šių paslaugų teikimo sutartyse, kuriose turi būti nurodomas paslaugos objektas ir paslaugos apimtis, jos teikimo laikas, prieinamumo ir patikimumo reikalavimai, funkcionalumo ir vykdymo reikalavimai, prieigos prie atitinkamos VLK informacinės sistemos ir elektroninės informacijos sukūrimo reikalavimai, stebėsenos reikalavimai, taip pat reikalavimai, keliami informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklais, saugai, įskaitant konfidencialumo ir informavimo apie elektroninės informacijos saugos incidentus, sutarties šalių veiksmų ribos ir atsakomybė, už sutarties vykdymą atsakingi sutarties šalių paskirti asmenys.

39. Informacinės sistemos administratorius atsako už programinių, techninių ir kitų prieigos prie atitinkamos VLK informacinės sistemos organizavimą, suteikimą ir panaikinimą taikomosios programinės įrangos priežiūros paslaugų teikėjui.

40. Paslaugų, užtikrinančių reikiamą atitinkamos VLK informacinės sistemos funkcionavimą, teikėjams suteikiamos tokios prieigos prie informacinės sistemos teisės, kurios yra būtinos sutartyje nustatytiems įsipareigojimams vykdyti ir neprieštarauja teisės aktų reikalavimams. Paslaugų teikėjo įgaliotam asmeniui teisės suteikiamos vadovaujantis VLK ir TLK informacinių išteklių privilegijuotųjų naudotojų veiksmų kontrolės tvarkos apraše, patvirtinto VLK direktoriaus įsakymu, nustatyta tvarka.

41. Pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui, ligonių kasų darbuotojas, atsakingas už sutarties vykdymą, informuoja atitinkamos VLK informacinės sistemos administratorių apie paslaugų teikėjo įgalioto darbuotojo prieigos prie Privilegijuotų naudotojų veiksmų kontrolės sistemos teisės panaikinimą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. VLK informacinių sistemų naudotojai, informacinių sistemų administratoriai ir informacinių sistemų saugos įgaliotinai už Taisyklių pažeidimus atsako teisės aktų nustatyta tvarka.

____

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 NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) valdomų informacinių sistemų naudotojų administravimo taisyklės (toliau – Taisyklės) nustato VLK ir teritorinių ligonių kasų (toliau – TLK, VLK ir TLK kartu vadinamos ligonių kasomis) bei kitų naudotojų (toliau – naudotojai) ir informacinių sistemų administratorių (toliau – administratoriai) įgaliojimus, teises ir pareigas tvarkant elektroninę informaciją.

2. Taisyklių tikslas – užtikrinti tinkamą naudotojų ir administratorių įgaliojimų, teisių bei pareigų valdymą Detalios paciento lygio sąnaudų apskaitos informacinės sistemoje ir kitose VLK informacinėse sistemose, kurios yra nurodytos VLK valdomų informacinių sistemų duomenų saugos nuostatuose, patvirtintuose VLK direktoriaus 2017 m. gruodžio 6 d. įsakymu Nr. 234 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo“.

3. Taisyklės taikomos informacinių sistemų naudotojams, administratoriams, informacinių sistemų saugos įgaliotiniams.

4. Taisyklės parengtos vadovaujantis:

4.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

4.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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“;

4.3. 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“;

4.4. 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“ (toliau – Elektroninės informacijos saugos reikalavimų aprašas);

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

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

4.6. kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacijos tvarkymą.

5. Taisyklėse vartojamos sąvokos atitinka Informacijos saugos nuostatuose, patvirtintuose VLK direktoriaus įsakymu, VLK valdomų informacinių sistemų duomenų saugos nuostatuose ir Taisyklių 4 punkte nurodytuose teisės aktuose vartojamas sąvokas.

6. Naudojimosi prieiga prie informacinių sistemų elektroninės informacijos principai:

6.1. elektroninės informacijos naudojimo būtinumo principas – elektronine informacija gali naudotis tik tie asmenys ir institucijos, kuriems tai būtina nustatytoms funkcijoms vykdyti;

6.2. elektroninės informacijos naudojimo leistinumo principas – naudotojams draudžiami visi veiksmai, kurių jiems atlikti neleidžia Taisyklės ir kiti teisės aktai, reglamentuojantys informacinių sistemų duomenų saugą, saugų elektroninės informacijos tvarkymą ir informacinių sistemų veiklos tęstinumo valdymą;

6.3. prieinamumo prie elektroninės informacijos ribojimo principas – teisė naudoti apibrėžtus informacinių sistemų duomenis suteikiama konkrečiam naudotojui, turinčiam unikalų jį identifikuojantį prisijungimo prie atitinkamos informacinės sistemos vardą ir slaptažodį;

6.4. elektroninės informacijos vientisumo principas – elektroninė informacija negali būti atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta. Šiam principui įgyvendinti informacinių sistemų elektroninė informacija turi būti perduodama saugiu duomenų perdavimo tinklu, ji turi būti apsaugota nuo pašalinio įsilaužimo, nuo asmenų, neturinčių prieigos prie informacinių sistemų teisės, bandymų koreguoti elektroninę informaciją;

6.5. duomenų konfidencialumo principas – elektroninė informacija turi būti tvarkoma vadovaujantis VLK valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis, patvirtintomis VLK direktoriaus įsakymu, ir neturi būti matoma pašaliniams asmenims. Šis principas turi būti įgyvendinamas priskiriant informacinių sistemų naudotojams atitinkamus vaidmenis ir teises;

6.6. duomenų teisingumo principas – informacinių sistemų duomenys turi būti pagrįsti įrodymais, turi būti žinomas jų pirminis šaltinis. Šį principą atitinkantys duomenys laikomi teisingais tol, kol jie nenuginčijami Lietuvos Respublikos įstatymų ir Europos Sąjungos teisės aktų nustatyta tvarka.

II SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

7. Prieigos prie VLK valdomų informacinių sistemų teisė suteikiama tik tiems ligonių kasų ir asmens sveikatos priežiūros įstaigų bei kitų įstaigų ar įmonių darbuotojams, kuriems ši prieiga reikalinga jų pareigybių aprašymuose nustatytoms funkcijoms vykdyti. Šie darbuotojai turi būti supažindinami su šiais dokumentais:

7.1. Taisyklėmis;

7.2. VLK valdomų informacinių sistemų duomenų saugos nuostatais;

7.3. VLK valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis;

7.4. VLK valdomų informacinių sistemų ir ryšio technologijų veiklos tęstinumo valdymo planu, patvirtintu VLK direktoriaus įsakymu.

8. Naudotojų pareigos ir įgaliojimai:

8.1. rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti informacinės sistemos duomenis tik savo tiesioginėms funkcijoms, nustatytoms pareigybių aprašymuose, vykdyti;

8.2. renkant, tvarkant, perduodant, saugant, naikinant ar kitaip naudojant informacinės sistemos duomenis vadovautis 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 (toliau – Reglamentas), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais saugų duomenų tvarkymą;

8.3. laikytis ligonių kasų Informacijos saugos valdymo sistemos (toliau – ISVS) dokumentuose nustatytų elektroninės informacijos saugos reikalavimų

8.4. naudotojams, įgaliotiems vykdyti tam tikras funkcijas, draudžiama atlikti veiksmus, kuriems jie neturi įgaliojimų;

8.5. naudojantis Informacinių technologijų ir informacinių sistemų pagalbos tarnybos informacine sistema (toliau – NAT IS) nedelsiant pranešti apie informacinių sistemų veiklos sutrikimus, apie esamus arba galimus elektroninės informacijos saugos reikalavimų pažeidimus bei kitus neteisėtus naudotojų veiksmus. Jeigu nėra galimybės pranešti apie tai per NAT IS, pranešti naudojantis kitomis informavimo priemonėmis;

8.6. susipažinti su informacinės sistemos saugos dokumentais;

8.7. pasirašyti nustatytos formos konfidencialumo pasižadėjimą;

8.8. laikytis visų informacinės sistemos saugos dokumentuose nustatytų reikalavimų.

9. Naudotojų teisės:

9.1. gauti visą informaciją, reikalingą savo funkcijoms informacinėse sistemose atlikti;

9.2. teikti siūlymus dėl papildomų informacinių sistemų funkcijų;

9.3. teikti siūlymus informacinės sistemos saugos įgaliotiniui dėl elektroninės informacijos saugos priemonių taikymo;

9.4. naudotis NAT IS pildant prašymą dėl techninės ir metodinės pagalbos, reikalingos vykdant jiems suteiktus įgaliojimus, jei nėra galimybių registruoti sutrikimą;

9.5. atlikti kitus veiksmus, numatytus ligonių kasų dokumentuose, reglamentuojančiuose informacinių sistemų saugą;

9.6. atitinkama tvarka pateikti prašymą dėl naudotojo prieigos prie informacinės sistemos sukūrimo arba atkūrimo, ar panaikinimo.

10. Administratorių pareigos ir įgaliojimai:

10.1. suteikti, panaikinti ar pakeisti prieigos teises naudotojams, atsižvelgiant į naudotojų ar jų vadovų pateiktus prašymus ir atliekamas funkcijas informacinėse sistemose;

10.2. suteikiant, panaikinant ar keičiant prieigos prie informacinių sistemų teises ir slaptažodžius, vadovautis Elektroninės informacijos saugos reikalavimų aprašo nuostatomis;

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

10.3. pagal NAT IS arba Naudotojų tapatybių ir teisių valdymo sistemoje (toliau – NTTVS) registruotą prašymą laiku atnaujinti pasikeitusius naudotojo duomenis;

10.4. pagal kompetenciją konsultuoti naudotojus dėl informacinės sistemos veikimo ir teikti jiems reikiamą techninę pagalbą;

10.5. diegti informacinės sistemos pakeitimus, užtikrinti tinkamą informacinės sistemos duomenų bazių ir posistemių (jei yra) funkcionavimą, atlikti kitus veiksmus, nuo kurių priklauso tinkamas informacinės sistemos programinės įrangos veikimas;

10.6. registruoti ir (ar), spręsti ir šalinti sutrikimus, susijusius su informacinės sistemos programinės įrangos veikimu;

10.7. vykdyti kitas VLK valdomų informacinių sistemų duomenų saugos nuostatuose ir (arba) Detalios paciento lygio sąnaudų apskaitos informacinės sistemos duomenų saugos nuostatuose, patvirtintuose VLK direktoriaus įsakymu, nustatytas funkcijas.

11. VLK administratorių teisės:

11.1. panaikinti naudotojo prieigą, jei buvo nustatyta, kad naudotojas nesilaiko VLK valdomų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse nustatytų reikalavimų;

11.2. panaikinti naudotojo prieigą, jeigu buvo nustatyta, kad naudotojas pažeidė Reglamentą ar Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nuostatas;

11.3. panaikinti naudotojo prieigą atsižvelgiant į vadovo prašymą, informuojantį, kad naudotojas nutraukia darbo santykius su ligonių kasomis arba pasikeičia naudotojo funkcijos ir joms vykdyti nereikia prieigos prie informacinės sistemos;

11.4. perduoti prieigos suteikimo naudotojams funkcijas TLK administratoriams (pagal kompetenciją ir poreikį) ir kontroliuoti jų veiksmus;

12. TLK administratorių teisės:

12.1. skaityti, kurti, atnaujinti, naikinti informacinės sistemos informaciją, tiesiogiai susijusią su TLK vykdomomis funkcijomis, tiesiogiai stebėti ir kontroliuoti TLK naudotojų veiksmus;

12.2. teikti informaciją VLK administratoriams apie informacinės sistemos programinės įrangos sutrikimus ir dalyvauti juos šalinant;

13. Informacinei sistemai administruoti gali būti paskirtas vienas ar keli administratoriai.

14. TLK administratorius, kuriam priskirta administruoti atitinkamą informacinę sistemą, negali vykdyti duomenų saugos įgaliotinio funkcijų.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINIŲ SISTEMŲ NAUDOTOJAMS KONTROLĖS TVARKA

15. Prieigos teisių prie atitinkamų informacinių sistemų suteikimo / panaikinimo VLK ir TLK naudotojams tvarka:

15.1. vadovaujantis ligonių kasų darbuotojo ar jo vadovo (ar jį pavaduojančio darbuotojo) pateiktu per NAT IS arba NTTVS prašymu, ligonių kasų darbuotojui suteikiamos, koreguojamos ar panaikinamos prieigos teisės;

15.2. ligonių kasų darbuotojas prašymą suderina su savo vadovu ar jį pavaduojančiu darbuotoju, užtikrinančiais, kad prašoma teisė į prieigą atitinka darbuotojo pareigybės aprašyme numatytas funkcijas;

15.3. ligonių kasų darbuotojo, kurio atliekamos funkcijos keičiasi arba su juo nutraukiami darbo santykiai, vadovas ar jį pavaduojantis darbuotojas turi užtikrinti, kad būtų panaikinta šio ligonių kasų darbuotojo teisė į prieigą. Jeigu darbuotojas NAT IS arba NTTVS nėra registravęs prašymo apie prieigos teisių panaikinimą, tai atlieka jo vadovas ar jį pavaduojantis darbuotojas;

15.4. informacinės sistemos saugos įgaliotinis, gavęs užduotį per NAT IS, patikrina, ar darbuotojas, kuriam prašoma suteikti teisę į prieigą, yra susipažinęs su informacijos saugos valdymo sistemos dokumentais ir pasirašęs nustatytos formos konfidencialumo pasižadėjimą, kurio forma pateikiama Informacijos saugos nuostatų, patvirtintų VLK direktoriaus įsakymu, 4 priede;

15.5. jeigu darbuotojas nėra susipažinęs su Taisyklių 15.4 papunktyje nurodytais dokumentais ir nėra pasirašęs konfidencialumo pasižadėjimo, atitinkamos informacinės sistemos informacijos saugos įgaliotinis būsimą naudotoją su jais supažindina, o naudotojas pasirašo konfidencialumo pasižadėjimą;

15.6. administratorius ne vėliau kaip kitą darbo dieną nuo informacinės sistemos saugos įgaliotinio patvirtinimo, kad darbuotojas yra supažindintas su informacijos saugos valdymo sistemos dokumentais, dienos suteikia šiam darbuotojui prieigą, ją atnaujina arba panaikina ir apie tai jį informuoja;

15.7. privalomojo sveikatos draudimo informacinės sistemos „Sveidra“, Finansų valdymo ir apskaitos informacinės sistemos, Europos duomenų mainų informacinės sistemos bei Eilių ir atsargų valdymo informacinės sistemos atveju prieigos teisė darbuotojui suteikiama, keičiama ar panaikinama naudojantis NTTVS ir vadovaujantis VLK ir TLK informacinių išteklių naudotojų tapatybių ir teisių valdymo tvarkos aprašu, patvirtintu VLK direktoriaus 2021 m. kovo 10 d. įsakymu Nr. 1K-87„Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų informacinių išteklių naudotojų tapatybių ir teisių valdymo tvarkos aprašo patvirtinimo“.

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

16. Asmens sveikatos priežiūros įstaigų ir kitų juridinių vienetų, su kuriais yra sudarytos sutartys dėl sveikatos priežiūros paslaugų, vaistų, medicinos pagalbos priemonių, ortopedijos techninių priemonių ir kt. kompensavimo iš Privalomojo sveikatos draudimo fondo biudžeto lėšų, naudotojų registravimo tvarka:

16.1. įstaigos vadovas ar jo įgaliotas asmuo užpildo Prašymo suteikti / panaikinti prieigą prie informacinės sistemos formą (1 priedas) (toliau – prašymas) ir elektroninėmis priemonėmis pateikia ją ligonių kasoms kartu su pasirašytu nustatytos formos Informacinės sistemos išorės naudotojo konfidencialumo pasižadėjimu (2 priedas);

16.2. įstaigos vadovas ar kitas įgaliotas asmuo, teikdamas prašymą, užtikrina, kad prašoma suteikti teisė į prieigą atitinka darbuotojo pareigybės aprašyme nustatytas funkcijas;

16.3. prašymas užregistruojamas Dokumentų valdymo sistemoje ir priskiriamas atsakingam už atitinkamos sutarties vykdymą ar atitinkamo projekto vykdymą ligonių kasų darbuotojui;

16.4. ligonių kasų darbuotojas, atsakingas už atitinkamos sutarties arba atitinkamo projekto vykdymą, gavęs užduotį per Dokumentų valdymo sistemą ir patikrinęs, ar prašymo teikėjui galima suteikti prieigą, pildo NAT IS prašymą suteikti teisę į prieigą;

16.5. jei išorės darbuotojui prieiga dėl pasikeitusių jo funkcijų yra nebereikalinga, įstaigos vadovas ar kitas įgaliotasis asmuo privalo ne vėliau kaip prieš 5 darbo dienas iki šio darbuotojo prieigos teisės panaikinimo dienos pateikti VLK prašymą šią teisę panaikinti;

16.6. informacinės sistemos saugos įgaliotinis, gavęs užduotį per NAT IS, patikrina, ar naudotojas, kuriam prašoma suteikti prieigos teisę, yra susipažinęs su atitinkamos informacinės sistemos dokumentais ir pasirašęs konfidencialumo pasižadėjimą;

16.7. jeigu būsimasis naudotojas nėra susipažinęs su atitinkamos informacinės valdymo dokumentais ir nėra pasirašęs konfidencialumo pasižadėjimo, atitinkamos informacinės sistemos informacijos saugos įgaliotinis būsimąjį naudotoją su jais supažindina, o būsimasis naudotojas pasirašo konfidencialumo pasižadėjimą;

16.8. VLK administratorius sugeneruoja saugaus prisijungimo raktą, skirtą jungtis saugiu virtualiu privataus tinklo (VPN) kanalu iki VLK tinklo;

16.9. administratorius ne vėliau kaip kitą darbo dieną nuo informacinės sistemos saugos įgaliotinio patvirtinimo, kad darbuotojas yra supažindintas su atitinkamos informacinės sistemos dokumentais, dienos suteikia šiam darbuotojui teisę į prieigą, ją atnaujina arba panaikina ir apie tai šį darbuotoją informuoja;

16.10. įstaigos ir įmonės, sudariusios sutartis su VLK ar TLK, kurios turi savo informacines sistemas ir nori gauti duomenis iš ligonių kasų valdomų informacinių sistemų per tinklinę sąsają (angl. *web service*), užpildo nustatytos formos Prašymą suteikti / panaikinti prieigą prie informacinės sistemos, naudojantis tinkline sąsaja (3 priedas).

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

17. Prisijungimo vardas ir slaptažodis negali būti saugomi arba perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais. Jie perduodami atskiromis priemonėmis.

18. Laikinasis slaptažodis gali būti perduodamas atviru tekstu, atskirai nuo prisijungimo vardo informacijos saugos įgaliotinio sprendimu, jeigu:

18.1. naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

18.2. nėra techninių galimybių naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

19. naudotojui prieigos teisės turi būti atnaujinamos pasikeitus prašyme nurodytiems darbuotojo duomenims (vardas, pavardė, pareigos, įstaiga).

20. Prieigos teisės gali būti sustabdomos, jeigu:

20.1. vykdomas naudotojo veiklos tyrimas ir jis nušalinamas nuo pareigų Lietuvos Respublikos valstybės tarnybos įstatymo, Lietuvos Respublikos darbo kodekso ar kitų teisės aktų pagrindais;

20.2. darbuotojas atliko neleistinus veiksmus ar pažeidė asmens duomenų apsaugos reikalavimus.

21. Administratorius privalo ne rečiau kaip kas 12 (dvylika) mėnesių patikrinti ne mažiau kaip 10 procentų naudotojų darbo vietų ir jose naudojamos programinės įrangos, prieigos teisių atitiktį slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimams.

22. Įstaigos vadovas (atsakingasis asmuo) privalo ne rečiau kaip kas 12 (dvylika) mėnesių patikrinti naudotojų turimas prieigos teises, jų aktualumą ir teisių turėjimo pagrindą.

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

23. Administratoriams prieigos teisės ir slaptažodžiai, skirti prisijungti prie informacinių sistemų, suteikiami vadovaujantis Elektroninės informacijos saugos reikalavimų aprašo nuostatomis.

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

24. Jeigu informacinę sistemą prižiūri / administruoja paslaugų teikėjas, tai prieigos ir slaptažodžiai prie informacinės sistemos suteikiami naudojantis Privilegijuotųjų naudotojų prieigos valdymo sistema ir vadovaujantis VLK ir TLK informacinių išteklių privilegijuotųjų naudotojų veiksmų kontrolės tvarkos aprašu, patvirtintu VLK direktoriaus 2015 m. birželio 8 d. įsakymu Nr. 1K-187 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų informacinių išteklių privilegijuotųjų naudotojų veiksmų kontrolės tvarkos aprašo patvirtinimo“.

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

25. Naudotojų tapatybė nustatoma pagal suteiktą unikalų informacinių sistemų naudotojo vardą, slaptažodį ir kitus duomenis.

26. Slaptažodžio sudarymo, saugojimo ir perdavimo taisyklės nustatomos vadovaujantis Elektroninės informacijos saugos reikalavimų aprašo nuostatomis.

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

27. Naudotojas, pirmą kartą jungdamasis prie informacinės sistemos, turi pasikeisti pirminio prisijungimo slaptažodį, o vėliau periodiškai jį keisti. Šio reikalavimo vykdymui užtikrinti pirmojo prisijungimo prie informacinės sistemos metu automatiniu būdu reikalaujama, kad naudotojas pakeistų pirminio prisijungimo slaptažodį (jeigu tokia galimybė numatyta informacinės sistemos programinėje įrangoje).

28. Naudotojas slaptažodį turi pakeisti ne rečiau kaip kas 3 mėnesius (jeigu to reikalauja informacinė sistema). Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (prisijungimo prie privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ slaptažodį – 10 simbolių), jis negali būti sudaromas iš naudotojo vardo ar pavardės.

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

29. Naudotojas privalo saugoti slaptažodį, jo neatskleisti ir nesudaryti kitų sąlygų juo naudotis kitiems asmenims, įskaitant tiesioginį vadovą.

30. Draudžiama naudotis kito naudotojo paskyra ir jo prisijungimo duomenimis.

31. Atostogų, laikino nedarbingumo ir kitais atvejais pavaduojant naudotoją ir esant būtinybei pasinaudoti informaciniais ištekliais, darbuotojo vadovas ar jį pavaduojantis darbuotojas Taisyklėse nustatyta tvarka turi pateikti prašymą dėl laikinos prieigos suteikimo. Prašyme turi būti nurodomos informacinė (-ės) sistema (-os), prie kurios (-ių) norima gauti prieigą, ir pateikiamas šio prašymo pagrindimas. Prieiga gali būti suteikta tik tokios apimties, kuri būtina laikinai nustatytoms

naudotojo funkcijoms vykdyti, ir tokiu būdu, kad informaciniai ištekliai naudotojo būtų pasiekiami naudojant savo paskyrą.

32. Naudotojams nuotolinė prieiga suteikiama pagal atskirą prašymą, pateikiamą tokiu pačiu būdu kaip ir prašymas suteikti teisę į prieigą.

33. Informacinių technologijų priežiūros paslaugas teikiančių naudotojų prieigos teisės valdomos VLK ir TLK informacinių išteklių privilegijuotųjų naudotojų veiksmų kontrolės tvarkos apraše nustatyta tvarka.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Taisyklės peržiūrimos kartu su kitais ISVS dokumentais ne rečiau kaip kartą per metus ir prireikus keičiamos VLK direktoriaus įsakymu.

Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos
valdomų informacinių sistemų
naudotojų administravimo taisyklių
1 priedas

(Prašymo suteikti / panaikinti prieigą prie informacinės sistemos forma)

____

(*Įmonės / įstaigos pavadinimas, juridinio asmens kodas*)

____

(*Data, reg. Nr.*)

Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos
Informacinių technologijų departamento direktoriui /
teritorinės ligonių kasos direktoriui

PRAŠYMAS SUTEIKTI / PANAIKINTI PRIEIGĄ PRIE INFORMACINĖS SISTEMOS

Prašau suteikti / panaikinti (*reikiamą pabraukti*) prieigą prie ____informacinės sistemos šiems mano atstovaujamos įmonės / įstaigos darbuotojams:

Eil. Nr.	Vardas, pavardė, asmens kodas*	Kontaktai (el. pašto adresas, tel. Nr.)**	Vykdoma funkcija***	Posistemis, prie kurio suteikiama prieiga, ir naudotojo teisės ****	Įstaigos ID	Data	
						nuo	iki (jei prieiga suteikia-ma termi-nuotam laikui)
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

* Asmens kodas nurodomas, jei prašoma suteikti prieigą prie privalomojo sveikatos draudimo informacinės sistemos „Sveidra“, Eilių ir atsargų valdymo informacinės sistemos, Europos duomenų mainų informacinės sistemos bei šių informacinių sistemų posistemių (asmens kodas naudojamas tik asmens tapatybei nustatyti, bet nenaudojamas prisijungti prie informacinės sistemos).

** Nurodomi kontaktai, būtini prisijungimo duomenims pateikti.

*** Nurodomos darbuotojo funkcijos, kurioms atlikti būtina prieiga prie informacinės sistemos.

**** Nurodomas informacinės sistemos posistemio pavadinimas ir naudotojo teisės.

____ _________________ __________________

(*Įmonės / įstaigos įgalioto asmens vardas, pavardė*) (*Parašas*) (*Data*)

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

Valstybinės ligonių kasos prie Sveikatos
apsaugos ministerijos valdomų
informacinių sistemų naudotojų
administravimo taisyklių
2 priedas

(Informacinės sistemos išorės naudotojo konfidencialumo pasižadėjimo forma)

INFORMACINĖS SISTEMOS IŠORĖS NAUDOTOJO KONFIDENCIALUMO PASIŽADĖJIMAS

____
(*Data, reg. Nr.*)

____
(*Įmonės / įstaigos pavadinimas, įmonės kodas, naudotojo vardas, pavardė*)

1. Aš suprantu, kad:

1.1. savo darbe tvarkysiu asmens ir (ar) asmens duomenis, kurie negali būti atskleisti ar perduoti neįgaliotiesiems asmenims ar institucijoms;

1.2. draudžiama perduoti neįgaliotiesiems asmenims slaptažodžius ir kitus duomenis, įgalinančius programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitaip sudaryti sąlygas susipažinti su asmens duomenimis;

1.3. netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę pagal Lietuvos Respublikos įstatymus.

2. Aš įsipareigoju:

2.1. saugoti asmens duomenų paslaptį;

2.2. tvarkyti asmens duomenis 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 (toliau – Reglamentas), Lietuvos Respublikos įstatymais ir kitais teisės aktais bei taisyklėmis, reglamentuojančiomis man patikėtas asmens duomenų tvarkymo funkcijas;

2.3. neatskleisti, neperduoti tvarkomos informacijos ir nesudaryti sąlygų sužinoti jos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek įmonės / įstaigos viduje, tiek už jos ribų;

2.4. pranešti savo vadovui apie bet kokią įtartiną situaciją, galinčią kelti grėsmę asmens duomenų saugumui;

2.5. saugoti informacinės sistemos slaptažodį, jį sudarant vadovautis ligonių kasų informacinių sistemų naudotojų administravimo taisyklėmis;

2.6. pranešti apie suteiktų prieigos teisių panaikinimą, jei nėra poreikio naudotis atitinkama informacine sistema.

3. Aš žinau, kad:

3.1. už šio pasižadėjimo nesilaikymą ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nuostatų pažeidimą turėsiu atsakyti pagal Lietuvos Respublikos įstatymus;

3.2. asmuo, patyręs žalą dėl neteisėto asmens duomenų tvarkymo arba kitų duomenų valdytojo / duomenų tvarkytojo veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą Reglamento, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų Lietuvos Respublikos teisės aktų nustatyta tvarka;

3.3. duomenų valdytojas ar duomenų tvarkytojas atlygina asmeniui padarytą žalą Lietuvos Respublikos teisės aktų nustatyta tvarka;

3.4. šis pasižadėjimas galios visą mano darbo laiką šioje įmonėje / įstaigoje (taip pat perėjus dirbti į kitą įmonę / įstaigą arba pasibaigus darbo santykiams).

Aš esu susipažinęs (-usi) su Reglamentu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų teisinę apsaugą, taip pat su Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos saugos dokumentų reikalavimais ir juos suprantu.

______________________	______________________	______________	_______________
(*Pareigos*)	(*Vardas, pavardė*)	(*Parašas*)	(*El. paštas*)

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

Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų naudotojų administravimo taisyklių
3 priedas

(Prašymo suteikti / panaikinti prieigą prie informacinės sistemos, naudojantis tinkline sąsaja, forma)

____
(*Įmonės / įstaigos pavadinimas, juridinio asmens kodas*)

Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos
Informacinių technologijų departamento direktoriui /
teritorinės ligonių kasos direktoriui

PRAŠYMAS SUTEIKTI / PANAIKINTI PRIEIGĄ PRIE INFORMACINĖS SISTEMOS, NAUDOJANTIS TINKLINE SĄSAJA

Prašau suteikti mano atstovaujamai įmonei / įstaigai prieigą prie informacinės sistemos____ ,
(nurodyti informacinės sistemos, posistemio pavadinimą)

skirtą šios įmonės / įstaigos informacinės sistemos______________________________________
(nurodyti įstaigos informacinės sistemos pavadinimą)

duomenims perduoti ir gauti, naudojantis tinkline sąsaja (angl. *web service*).

______________________________________ ____________________ ________________
(*Įgaliotojo asmens vardas, pavardė, pareigos*) (*Parašas*) (*Data*)

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

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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai	Atsakingi vykdytojai	Terminai
	1.5 Nustatoma, ar pasiekiama serverinė. Jei ne, toliau atliekami veiksmai, numatyti 1.6 papunktyje. Jei taip, toliau atliekami veiksmai, numatyti 1.7 papunktyje.	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo
	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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai	Atsakingi vykdytojai	Terminai
2. Nepasiekiama serverinė (dėl gaisro pastato dalyje, kurioje yra duomenų centras, dėl inžinerinių sistemų gedimo (rezervinės elektros maitinimo, kondicionavimo ir vėdinimo ar pan.)	2.1. Nustatoma, kad serverinė yra nepasiekiama.	Veiklos atkūrimo grupė	Per 30 min. po incidento nustatymo
	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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
3. Nepasiekiama techninė įranga (dėl techninės įrangos gedimo, kai 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)	3.1. 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
	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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai	Atsakingi vykdytojai	Terminai
	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
	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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	**Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai**	**Atsakingi vykdytojai**	**Terminai**
	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
	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	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

Elektroninės informacijos ar kibernetinės saugos incidentas (toliau – incidentas)	Veiklos tęstinumo valdymo (atkūrimo) veiksmai / incidentų šalinimo scenarijai	Atsakingi vykdytojai	Terminai
išorinėmis sistemomis)	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
	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.	Veiklos tęstinumo valdymo grupė	Per vieną darbo valandą po situacijos analizės

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 6.6 papunktyje.		
	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
	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

2.
Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. 1K-246, 2023-09-25, paskelbta TAR 2023-09-25, i. k. 2023-18632

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