PATVIRTINTA
VšĮ Klaipėdos rajono savivaldybės Gargždų
ligoninės vyriausiosios gydytojos
2019 m. kovo 27 d. įsakymu Nr. 25

VŠĮ KLAIPĖDOS RAJONO SAVIVALDYBĖS GARGŽDŲ LIGONINĖS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės informacinės sistemos veiklos tęstinumo valdymo plano (toliau – valdymo planas) tikslas – nustatyti VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės (toliau – Įstaiga) darbuotojų veiksmus esant elektroninės informacijos saugumo incidentui informacinėje sistemoje (toliau – IS), kurio metu gali kilti pavojus IS techninės, programinės įrangos funkcionavimui ir duomenims.

2. Valdymo planas parengtas vadovaujantis:

2.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

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

2.3. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas; toliau – BDAR);

2.4. Lietuvos standartais:

2.4.1. LST ISO/IEC 27001:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos;

2.4.2. LST ISO/IEC 27002:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas;

2.5. kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą, duomenų tvarkytojų veiklą ir duomenų saugumo valdymą.

3. Valdymo plane vartojamos sąvokos:

Elektroninė informacija – informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija.

Elektroninės informacijos sauga – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

Elektroninės informacijos saugos politika (toliau – saugos politika) – pagrindiniai elektroninės informacijos saugos užtikrinimo ir valdymo principai, reikalavimai, į kuriuos atsižvelgiant turi būti derinami IS veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai.

IS administratorius (toliau – administratorius) – darbuotojas, dirbantis pagal darbo sutartį, prižiūrintis IS ir (ar) jos infrastuktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą.

IS saugos įgaliotinis (toliau – saugos įgaliotinis) – darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą IS.

IS naudotojas – darbuotojas, dirbantis pagal darbo sutartį, ar kitas asmuo, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

Kitos valdymo plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, kituose Lietuvos Respublikos įstatymuose ir Lietuvos standartuose LST ISO/IEC 27001:2017 ir LST ISO/IEC 27002:2017.

4. Valdymo planas įsigalioja, kai dėl rizikos veiksnių nurodytų VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės informacinės sistemos veiklos atkūrimo detaliajame plane (toliau – veiklos atkūrimo detalusis planas) (1 priedas), įvyksta saugumo incidentas, dėl kurio sutrinka IS veiklos tęstinumas ir tampa aišku, kad atkurti IS veikimą per 8 val. nepavyks.

5. Už valdymo plano įgyvendinimo organizavimą atsakingas Įstaigos vadovas ir jo įgalioti asmenys.

6. Valdymo plane nurodytomis IS veiklos tęstinumo procedūromis yra siekiama šių tikslų:

6.1. paskelbus apie saugumo įvykį, sutrikdžiusį IS veiklą, per trumpiausią terminą atkurti IS ir jos posistemių veiklą;

6.2. sustabdyti veiklą, kuri nėra gyvybiškai svarbi, kol bus visiškai atkurtas pagrindinių IS ir jos posistemių veiklos tęstinumas;

6.3. sušvelninti bet kokio saugumo įvykio, nurodyto veiklos atkūrimo detaliajame plane, poveikį, atliekant šiame plane nustatytus atsakomuosius veiksmus;

6.4. sumažinti nesusipratimų ir klaidingos informacijos kiekį, sudarant aiškų veiklos atkūrimo detalųjį planą ir jame įvardijant atsakingus asmenis.

7. Kiekvienas naudotojas, pastebėjęs susidariusią situaciją, kuri kelia grėsmę IS veiklos tęstinumui, privalo:

7.1. informuoti Įstaigos vadovą apie pastebėtą situaciją, keliančią grėsmę IS veiklos tęstinumui;

7.2. rūpintis asmeniniu saugumu, vadovautis avarijos likvidavimo procedūromis, vykdyti pagalbos tarnybų nurodymus;

7.3. teikti pagalbą kitiems naudotojams nerizikuodamas savo sveikata;

7.4. tęsti veiklą, kiek tai įmanoma susidariusios situacijos sąlygomis;

7.5. pagal kompetenciją užtikrinti informacijos saugumą ir kokybę;

7.6. vykdyti IT kompanijos, prižiūrinčios Įstaigos IT ūkį, nurodymus;

7.7. išsaugoti IS veiklai gyvybiškai svarbius duomenis, kad IS veiklos tęstinumas vėliau galėtų būti atkurtas.

8. Valdymo planas yra parengtas ir taikomas Įstaigos patalpoms, esančioms Gabijos g. 32, Vilnius, kuriose yra Įstaigos tarnybinės stotys ir saugomi, valdomi ir tvarkomi IS duomenys.

9. Kriterijai, pagal kuriuos nustatoma, kad IS veikla atkurta:

9.1. veikia visa IS darbui reikalinga infrastruktūra;

9.2. naudotojams prieinamos ir be kritinių klaidų veikia visos IS funkcijos;

9.3. atnaujinami IS duomenys;

9.4. išsaugomi atnaujinti IS duomenys;

9.5. daromos IS duomenų atsarginės kopijos.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

10. Įstaigos IS veiklos tęstinumo valdymo grupės (toliau – Valdymo grupė) sudėtis:

10.1. direktorius (Valdymo grupės vadovas);

10.2. IS sistemas Įstaigoje prižiūrinti samdoma Įstaiga ar Įstaigos darbuotojas;

10.3. kiti direktoriaus įsakymu paskirti Įstaigos darbuotojai.

11. Valdymo grupės funkcijos:

11.1. IS elektroninės informacijos saugos incidentų analizė ir sprendimų IS veiklos tęstinumo valdymo klausimais priėmimas;

11.2. bendravimas su IS naudotojais;

11.3. bendravimas su teisėsaugos ir kitomis institucijomis, kitomis interesų grupėmis;

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

11.5. bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

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

11.7. IS elektroninės informacijos fizinės saugos užtikrinimo kontrolė, įvykus IS elektroninės informacijos saugos incidentui;

11.8. logistikos organizavimas (žmonių, daiktų, įrangos gabenimo organizavimas ir jų gabenimas);

11.9. IS veiklos atkūrimo priežiūra ir koordinavimas;

11.10. kitos Valdymo grupei pavestos funkcijos.

12. Įstaigos IS veiklos atkūrimo grupės (toliau – Atkūrimo grupė) sudėtis:

12.1. direktorius (Valdymo grupės vadovas);

12.2. IS administratoriai;

12.3. kiti direktoriaus įsakymu paskirti Įstaigos darbuotojai.

13. Atkūrimo grupės funkcijos:

13.1. IS tarnybinių stočių veiklos atkūrimo organizavimas;

13.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

13.3. IS elektroninės informacijos atkūrimo organizavimas;

13.4. IS taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

13.6. kitos Atkūrimo grupei pavestos funkcijos.

14. Įvykus IS elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma IS techninė ir programinė įranga atliekami šie IS veiklos atkūrimo veiksmai:

14.1. IS administratorius apie IS elektroninės informacijos saugos incidentą nedelsdamas informuoja Įstaigos direktorių ir Valdymo bei Atkūrimo grupes;

14.2. IS administratorius informaciją apie IS informacijos saugos incidentą registruoja ir teisės aktų nustatyta tvarka organizuoja jo tyrimą.

14.3. IS administratorius atkuria IS techninės ir programinės įrangos veikimą, elektroninių ryšių tinklo veiklą, IS duomenis, IS techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai nedelsdamas informuoja Įstaigos vadovą;

14.4. IS administratorius organizuoja žalos IS duomenims, IS techninei, programinei įrangai vertinimą, IS veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą nustatyta tvarka.

15. Atsarginių patalpų, naudojamų IS veiklai atkurti IS elektroninės informacijos saugos incidento atveju, adresas ir būdai, kaip iki jų nuvykti, yra pateikti Valdymo plano 2 priede.

16. Valdymo ir Atkūrimo grupės ne rečiau negu kartą per metus organizuoja šių dviejų grupių susitikimą, kuriame aptariama esama situacija ir suderinami galimi jos pagerinimo būdai.

17. IS administratorius:

17.1. kasmet iki gruodžio 15 d. Valdymo grupei pateikia informaciją apie esamą IS saugumo būklę bei tais metais atliktus veiksmus, susijusius su IS sauga;

17.2. informuoja Įstaigos vadovą apie IS įvykusius kibernetinius incidentus, dėl kurių kilo arba galėjo kilti grėsmė Įstaigos IS duomenims, IS techninės ir programinės įrangos funkcionavimui, ir kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, jų galimas priežastis, veiksmus, kurių imtasi ir (arba) planuojama imtis šalinant šiuos incidentus, bei pasekmes.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

18. Veiklos tęstinumo vykdymui užtikrinti yra naudojama detali ir aktuali informacija:

18.1. Informaciją apie IS techninę ir programinę įrangą ir jos parametrus, aprašytus IS specifikacijose, parengia ir saugo IS administratorius.

18.2. Patalpų brėžinius ir šiose patalpose esančios įrangos bei komunikacijų sąrašą parengia ir saugo Įstaigos vadovas ar jo įgaliotas darbuotojas.

18.3. Telekomunikacijų tinklo fizinio ar loginio sujungimo schemas parengia ir saugo IS administratorius.

18.4. Duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutartis parengia ir saugo Įstaigos vadovas ar jo įgaliotas darbuotojas.

18.5. Programinės įrangos laikmenos ir laikmenos su atsarginėmis duomenų kopijomis saugomos atsarginėse patalpose, naudojamose IS veiklai atkurti IS elektroninės informacijos saugos incidento atveju. Atsarginės duomenų kopijos yra perkeliamos į saugojimo vietą kartą per mėnesį. Už atsarginių kopijų saugojimą atsako Įstaigos vadovas ar IS administratorius.

18.6. Įstaigos darbuotojų sąrašai, kuriuose nurodyti darbuotojų darbo telefonai, o Valdymo grupės ir Atkūrimo grupės narių – mobiliųjų ir namų telefonų numeriai bei gyvenamosios vietos adresai, parengia ir saugo Įstaigos vadovas ar jo įgaliotas darbuotojas.

19. Jeigu informacinės sistemos veiklai atkurti susidaro ekstremali situacija, kai IS administratorius negali dėl komandiruotės, ligos ar kitų priežasčių operatyviai atvykti į darbo vietą, jį pavaduojančio asmens minimalus kompetencijos ar žinių lygis, negali būti žemesnis už IS administratoriui keliamų reikalavimų lygį.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

20. Valdymo plano veiksmingumo išbandymo data nustatoma kiekvienų metų sausio mėnesį. Nustatytą dieną imituojamas IS elektroninės informacijos saugos incidentas. Jo metu už IS elektroninės informacijos saugos incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus.

21. Pagal bandymų rezultatus IS administratorius parengia IS veiklos tęstinumo valdymo plano bandymo ataskaitą (Valdymo plano 3 priedas) (toliau – Ataskaita), kurioje yra apibendrinami atliktų bandymų rezultatai, akcentuojami pastebėti IS trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės.

22. IS administratorius nuolat kontroliuoja Ataskaitoje nurodytų prevencinių priemonių įgyvendinimą.

23. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Įstaigos informacinių
sistemų veiklos tęstinumo
valdymo plano
1 priedas

VŠĮ KLAIPĖDOS RAJONO SAVIVALDYBĖS GARGŽDŲ LIGONINĖS INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Situacija	Siūlomi veiksmai	Vykdytojai
Gautas pranešimas apie IS elektroninės informacijos saugos incidentą	1. Pranešama Įstaigos direktoriui, jo pavaduotojams. 2. Pranešama Veiklos tęstinumo valdymo grupei. 3. Surenkama informacija apie neveikiančias arba apgadintas IS, patalpas arba patirtą kitokią žalą.	IS administratorius
	Skelbiama ekstremalioji situacija	Įstaigos vadovas
	Prireikus parengiami ir išplatinami informaciniai pranešimai interesų grupėms: 1. visiems Įstaigos darbuotojams. Informaciniame pranešime turi būti pateikiamos rekomendacijos, kaip elgtis esant ekstremaliai situacijai, nurodomi atsakingi darbuotojai ir jų kontaktinė informacija; 2. IS tvarkytojams, duomenų gavėjams; 3. viešosios informacijos skleidėjams; 4. teisėsaugos institucijoms.	Veiklos tęstinumo valdymo grupė
Nustatyta IS padaryta žala	1. Parengiamas priemonių planas kilusiam pavojui užkirsti. 2. Sudaroma Veiklos atkūrimo grupė, atsižvelgiant į IS pažeidimus.	Veiklos tęstinumo valdymo grupė
Nustatytas patalpų pažeidimas ir (ar) pavojus darbuotojų sveikatai arba gyvybei	1. Darbuotojai evakuojami iš Įstaigos patalpų. 2. Pranešama atitinkamoms tarnyboms.	Veiklos tęstinumo valdymo grupė
Nustatyti IS pažeidimai, dėl kurių jos negali funkcionuoti	1. Priimamas sprendimas atkurti IS rezerviniame duomenų centre (jei toks numatytas). 2. Organizuojamas pažeistų patalpų remontas, atstatymo darbai, komunalinių komunikacijų pajungimas.	Veiklos tęstinumo valdymo grupė
	Rezerviniame nuotoliniame duomenų centre organizuojamas veiklos atkūrimas	Veiklos atkūrimo grupė
Nustatytas IS techninės,	1. Parengiama atkūrimui būtina minimali techninė ir programinė įranga.	IS administratorius

Situacija	Siūlomi veiksmai	Vykdytojai
programinės įrangos ir (arba) duomenų praradimas	2. Atkuriama techninės, programinės įrangos veikla. 3. Atkuriami prarasti duomenys.	
Nustatytas ryšio linijų sutrikimas, dėl kurio nustoja funkcionuoti IS	1. Nustatomos ryšio sutrikimo priežastys. Šalinami ryšio sutrikimai. 2. Ryšio paslaugų tiekėjas užklausiamas dėl įvykusio sutrikimo pašalinimo trukmės prognozės. 3. Aktyvuojama rezervinė ryšio priemonė (jei tokia numatyta).	IS administratorius
	Pranešama atitinkamų tarnybų atsakingiems asmenims ir duomenų gavėjams.	Veiklos tęstinumo valdymo grupė
Nustatytas techninės įrangos sugadinimas, dėl kurio nustoja funkcionuoti IS	1. Priimamas sprendimas dėl techninės įrangos perskirstymo. 2. Prireikus kreipiamasi į techninės įrangos tiekėjus dėl sugadintos įrangos remonto arba dėl naujos techninės įrangos įsigijimo.	Veiklos tęstinumo valdymo grupė
	Perskirstoma esama techninė įranga ir kiti ištekliai, reikalingi IS veiklai užtikrinti	Veiklos atkūrimo grupė
Nustatytas programinės įrangos sugadinimas, dėl kurio nustoja funkcionuoti IS	Priimamas sprendimas dėl programinės įrangos įsigijimo	Veiklos tęstinumo valdymo grupė
	Iš esamų arba įsigytų programinės įrangos kopijų atkuriama sugadinta ar prarasta programinė įranga	IS administratorius
Nustatytas duomenų sugadinimas ar praradimas, dėl kurio nustoja funkcionuoti IS	1. Atkuriami prarasti duomenys. 2. Nepasisekus visiškai atkurti sugadintų ar prarastų duomenų iš atsarginių duomenų kopijų, Veiklos atkūrimo grupė organizuoja trūkstamų duomenų įkėlimą iš naujo.	Veiklos atkūrimo grupė; IS administratorius
Priežastys, kurios sukėlė ekstremaliąją situaciją, išnyksta ar yra pašalinamos, arba atkuriamas IS minimalus funkcionalumas.	Atšaukiama ekstremali situacija	Įstaigos vadovas
	Užpildoma IS veiklos tęstinumo valdymo eigos (plano bandymo) ataskaita (3 priedas).	IS administratorius
	Apie atšauktą ekstremalią situaciją prireikus pranešama interesų grupėms.	Veiklos atkūrimo grupė

Įstaigos informacinių sistemų
veiklos tęstinumo valdymo plano
2 priedas

ATSARGINIŲ PATALPŲ, NAUDOJAMŲ INFORMACINIŲ SISTEMŲ VEIKLAI ATKURTI ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTO ATVEJU, ADRESAS IR BŪDAI, KAIP IKI JŲ NUVYKTI

Atsarginių patalpų adresas: _____

Atsarginių patalpų vieta žemėlapyje:

(žemėlapio vaizdas)

_____

Įstaigos informacinių sistemų
veiklos tęstinumo valdymo
plano
3 priedas

INFORMACINIŲ SISTEMŲ IR REGISTRŲ VEIKLOS TĘSTINUMO VALDYMO EIGOS (PLANO BANDYMO) ATASKAITA

_____

(Veiklos tęstinumo valdymo grupės susitikimo data ir dokumento numeris)

Ekstremaliosios situacijos bandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai:

1. _____
2. _____
3. _____
4. ... _____

Ekstremaliosios situacijos apibūdinimas:

_____

_____

Informacinės sistemos, kurias paveikė ekstremalioji situacija:

_____

_____

Ekstremaliosios situacijos valdymo eiga:

_____

_____

Rasti Plano trūkumai:

_____

_____

Pasiūlymai keisti arba papildyti Planą:

_____

_____

_____ _____

(vardas, pavardė) (parašas)

_____ _____

(vardas, pavardė) (parašas)

_____ _____

(vardas, pavardė) (parašas)

_____