PATVIRTINTA
Viešosios įstaigos Vilkpėdės ligoninės
direktoriaus
2017 m. birželio 30 d. įsakymu Nr. 49

VIEŠOSIOS ĮSTAIGOS VILKPĖDĖS LIGONINĖS INFORMACINIŲ IŠTEKLIŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Vilkpėdės ligoninės (toliau – VšĮ Vilkpėdės ligoninė) informacinių išteklių (toliau – VLII) veiklos tęstinumo valdymo plano (toliau - Valdymo planas) tikslas - nustatyti VLII saugos įgaliotinio (kibernetinio saugumo vadovo), VLII administratoriaus ir kitų asmenų veiksmus ir procedūras, esant elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus VLII elektroninei informacijai, VLII techninės ir programinės įrangos funkcionavimui.

2. Valdymo planas parengtas vadovaujantis:

2.1. 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 ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

2.2. Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;

2.3. Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

2.4. Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“;

2.5. VLII duomenų saugos nuostatais.

2.6. Valdymo plane vartojamos sąvokos atitinka šio plano 2 punkte nurodytuose teisės aktuose vartojamas sąvokas.

3. Valdymo planas įsigalioja , jei:

3.1. pastebimas elektroninės informacijos saugos incidentas, darantis ar galintis padaryti įtaką VLII elektroninės informacijos vientisumui, konfidencialumui ar prieinamumui;

3.2. bent vienas iš VLII komponentų neveikia ilgiau nei keturias valandas ir nėra nustatyta nesklandumų priežastis arba priežastis yra nustatyta, tačiau numatomas gedimo šalinimo laikas yra ilgesnis nei 24 valandos.

4. VLII elektroninės informacijos saugos (kibernetinio saugumo) incidentų tyrimas atliekamas pagal VLII elektroninės informacijos saugos (kibernetinio saugumo) incidentų tyrimų tvarką (Valdymo plano 1 priedas).

5. Įvykę VLII elektroninės informacijos saugos (kibernetinio saugumo) incidentai registruojami VLII elektroninės informacijos saugos incidentų registravimo žurnale (Valdymo plano 2 priedas)

6. VLII administratoriaus (-ių), VLII saugos įgaliotinio (kibernetinio saugumo vadovo), naudotojų ir kitų asmenų įgaliojimai ir veiksmai elektroninės informacijos saugos incidento metu yra nurodyti VLII veiklos atkūrimo detaliajame plane (Valdymo plano 3 priedas).

7. Valdymo plano vykdymas VLII valdytojui, administratoriams, saugos įgaliotiniui (kibernetinio saugumo vadovui), naudotojams yra privalomas elektroninės informacijos saugos incidentų atveju, kurių metu gali kilti pavojus VLII elektroninei informacijai. VLII techninės.

programinės įrangos funkcionavimui.

8. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami ir VLII veikla atkuriama VLII valdytojo lėšomis.

9. VLII veikla laikoma atkurta, jeigu tenkinami šie kriterijai:

9.1. veikia visi VLII komponentai;

9.2. galimas VLII elektroninės informacijos atnaujinimas;

9.3. galimas VLII elektroninės informacijos išsaugojimas;

9.4. galimi elektroninės informacijos mainai tarp VLII ir kitų registrų bei informacinių sistemų pagal su šių informacinių sistemų valdytojais sudarytose elektroninės informacijos teikimo sutartyse numatytus būdus, terminus ir apimtį;

9.5. galimas VLII prieinamumas visų autorizuotų naudotojų atžvilgiu;

9.6. pašalintos kibernetinio incidento atsiradimo priežastys ir likviduoti padariniai.

10. VLII veikla turi būti atkurta per laikotarpį, ne ilgesnį nei 24 valandų, nuo VLII elektroninės informacijos incidento pastebėjimo.

II. SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. VLII elektroninės informacijos saugos (kibernetinio saugumo) incidentams valdyti ir veiklos atstatymui organizuoti VšĮ Vilkpėdės ligoninėje sudaryta – Veiklos tęstinumo valdymo ir atkūrimo grupė (toliau – Valdymo ir atkūrimo grupė).

12. Valdymo ir atkūrimo grupės tikslai – tirti elektroninės informacijos saugos (kibernetinio saugumo) incidentus, ieškoti priemonių ir būdų sukeltiems padariniams bei žalai likviduoti, užtikrinti VLII veiklos tęstinumą, likviduojant elektroninės informacijos saugos (kibernetinio saugumo) incidentus.

13. Valdymo ir atkūrimo grupės sudėtis:

13.1. VšĮ Vilkpėdės ligoninės direktorė – Valdymo grupės vadovė;

13.2. VšĮ Vilkpėdės ligoninės Ūkio skyriaus vedėjas-IT administratorius – Valdymo ir atkūrimo grupės vadovo pavaduotojas;

13.3. VšĮ Vilkpėdės ligoninės Raštinės vedėja

13.4. VšĮ Vilkpėdės ligoninės Personalo vadovė;

13.5. VšĮ Vilkpėdės ligoninės Vyriausioji buhalterė

14. Valdymo ir atkūrimo grupės funkcijos:

14.1. situacijos analizė ir sprendimų VLII veiklos tęstinumo valdymo klausimais priėmimas;

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

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

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

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

14.6. VLII elektroninės informacijos fizinė sauga įvykus elektroninės informacijos saugos incidentui;

14.7. logistika (žmonių, daiktų, įrangos gabenimas ir organizavimas);

14.8. VLII veiklos atkūrimo priežiūra ir koordinavimas;

14.9. VLII tarnybinių stočių veikimo atkūrimo organizavimas (Ūkio skyriaus vedėjas-IT administratorius, Raštinės vedėja);

14.10. kompiuterių tinklo veikimo atkūrimo organizavimas (Ūkio skyriaus vedėjas-IT administratorius, Raštinės vedėja);

14.11. VLII elektroninės informacijos atkūrimo organizavimas (Ūkio skyriaus vedėjas-IT administratorius, Raštinės vedėja);

14.12. taikomųjų programų tinkamo veikimo atkūrimo organizavimas (Ūkio skyriaus vedėjas-IT administratorius, Raštinės vedėja);

14.13. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas (Ūkio skyriaus vedėjas-IT administratorius, Raštinės vedėja);

15. Įvykus elektroninės informacijos saugos incidentui vadovaujamasi VLII elektroninės informacijos saugos (kibernetinio saugumo) incidentų tyrimų tvarka (Valdymo plano 1 priedas) bei VLII veiklos atkūrimo detaliuoju planu (Valdymo plano 3 priedas), VLII atkuriami šiuo eiliškumu:

15.1. Tarnybinių stočių veikimo atkūrimas;

15.2. Duomenų bazių veikimo atkūrimas;

15.3. Svetainių veikimo atkūrimas;

15.4. Kompiuterinio tinklo veikimo atkūrimas;

15.5. Taikomųjų programų veikimo atkūrimas;

15.6. Kompiuterizuotų darbo vietų veikimo atkūrimas ir prijungimas prie kompiuterių tinklo.

16. Elektroninės informacijos saugos (kibernetinio saugumo) incidento metu sunaikinta ar sugadinta įranga įsigyjama viešųjų pirkimų būdu. Laikotarpiu, iki reikiamos įrangos įsigijimo viešųjų pirkimų būdu, VLII veiklos atkūrimui naudojama rezerve esanti įranga.

17. Elektroninės informacijos saugos (kibernetinio saugumo) incidento metu praradus aukštos kvalifikacijos specialistus, laikinai, iki bus priimti nauji specialistai, pasitelkiami kiti kvalifikuoti asmenys.

18. Valdymo ir atkūrimo grupės nariai bendravimui naudoja elektroninį paštą, telefonus, mobiliojo ryšio ir kitas tuo metu prieinamas ryšio priemones.

III. SKYRIUS
APRAŠOMOSIOS NUOSTATOS

19. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) parengia ir esant reikalui peržiūri ir atnaujina:

19.1. informacinių technologijų įrangos, jos parametrų ir už jos priežiūrą atsakingų asmenų sąrašus bei minimalaus kompetencijos ar žinių lygio, reikalingo VLII veiklos atkūrimui nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, aprašus;

19.2. minimalaus informacinių technologijų įrangos funkcionalumo, pakankamo užtikrinti VLII valdytojo poreikius elektroninės informacijos saugos incidento metu, specifikaciją;

19.3. kiekvieno pastato aukšto patalpų brėžinius ir šiose patalpose esančią įrangą bei komunikacijas:

19.3.1. tarnybines stotis;

19.3.2. kompiuterių tinklo ir telefonų tinklo mazgus;

19.3.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

19.3.4. elektros įvedimo pastate vietas;

19.4. kompiuterių tinklo fizinio ir loginio sujungimo schemas;

19.5. elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių, taip pat atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigų sąrašus;

19.6. programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vietą ir šių laikmenų perkėlimo į saugojimo vietą laiką ir sąlygų aprašą;

19.7. Valdymo ir atkūrimo grupės narių sąrašą su kontaktiniais duomenimis, leidžiantį pasiekti šiuos asmenis bet kuriuo metu.

20. Už aukščiau paminėtų dokumentų kopijų saugojimą atsakingas VLII administratorius.

IV. SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

21. Valdymo planas turi būti išbandytas ne rečiau kaip kartą per metus.

22. Valdymo plano išbandymo data nustatoma kiekvienų metų sausio mėnesį. Nustatytą dieną imituojamos nenumatytos situacijos, jų metu už elektroninės informacijos saugos (kibernetinio saugumo) incidentų padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo

veiksmus. Iš atsarginių VLII elektroninės informacijos kopijų, atkuriama VLII elektroninė informacija.

23. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) yra atsakingas už ataskaitos apie Valdymo plano išbandymo rezultatus ir pastebėtus trūkumus parengimą (Valdymo plano 5 priedas).

24. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) kontroliuoja ataskaitoje nurodytų trūkumų šalinimo priemonių įgyvendinimą.

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

Viešosios įstaigos Vilkpėdės ligoninės
informacinių išteklių veiklos tęstinumo
valdymo plano
1 priedas

VLII ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) INCIDENTŲ TYRIMO TVARKA

1. VLII naudotojas, pastebėjęs saugą reglamentuojančiuose dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones arba įtaręs, kad su VLII duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai VLII administratoriui.

2. VLII administratorius nedelsdamas turi imtis veiksmų elektroninės informacijos saugos (kibernetinio saugumo) incidento priežastims nustatyti.

3. VLII administratorius pasinaudojęs VLII veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką, veiksmus, atliktus su VLII programine įranga ir (ar) duomenimis bei kategoriją remdamasis kibernetinių incidentų kategorijų sąrašu (Valdymo plano 4 priedas).

4. Nustačius, kad VLII naudotojo pastebėti pažeidimai yra pagrįsti, VLII administratorius privalo nedelsdamas imtis veiksmų elektroninės informacijos saugos (kibernetinio saugumo) incidentui sustabdyti ir apie incidentą pranešti VLII saugos įgaliotiniui (kibernetinio saugumo vadovui).

5. VLII saugos įgaliotinis (kibernetinio saugumo vadovas), gavęs pranešimą apie vykdomus neteisėtus veiksmus su VLII arba su VLII tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras ir apie tai informuoja Valdymo ir atkūrimo grupės vadovą.

6. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) informaciją apie elektroninės informacijos saugos incidentą įrašo į VLII elektroninės informacijos saugos incidentų registravimo žurnalą (Valdymo plano 2 priedas).

7. Valdymo ir atkūrimo grupės vadovas organizuoja nenumatytos situacijos įvertinimą ir priima sprendimą dėl nenumatytos situacijos padarinių šalinimo;

8. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) organizuoja žalos VLII duomenims, techninei, programinei įrangai vertinimą, koordinuoja techninės, sisteminės ir taikomosios programinės įrangos VLII veiklai atkurti įsigijimą, kibernetinio incidento atveju organizuoja informacijos, kurią yra būtina pateikti Kibernetinio saugumo centrui (toliau - Centras) surinkimą ir pateikimą;

9. Kibernetinio incidento atveju VLII saugos įgaliotinis (kibernetinio saugumo vadovas) Centrui praneša apie:

9.1. didelės reikšmės kibernetinį incidentą – ne vėliau kaip per **vieną valandą** nuo jo nustatymo;

9.2. vidutinės reikšmės kibernetinį incidentą – ne vėliau kaip per **4 valandas** nuo jo nustatymo;

9.3. nereikšmingą kibernetinį incidentą – ne vėliau kaip per **7 dienas** nuo jo nustatymo;

10. Pranešime apie didelės ir vidutinės reikšmės kibernetinį incidentą VLII saugos įgaliotinis (kibernetinio saugumo vadovas) nurodo:

10.1. kibernetinio incidento grupė;

10.2. trumpas kibernetinio incidento apibūdinimas;

10.3. tikslus laikas, kada kibernetinis incidentas įvyko ir nustatytas;

10.4. kibernetinio incidento kategorija;

10.5. kibernetinio incidento šalinimo tvarka (turi būti nurodyta, ar tai prioritetas, ar ne);

11. Pranešime apie nereikšmingą kibernetinį incidentą turi būti pateikta informacija apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo pateikimo dienos, skaičių;

12. Centrui turi būti pateikiamas vertinimas:

12.1. didelės reikšmės kibernetinio incidento – ne vėliau kaip per **2 valandas** nuo jo nustatymo;

12.2. vidutinės reikšmės kibernetinio incidento – ne vėliau kaip per **24 valandas** nuo jo nustatymo;

13. Didelės ir vidutinės reikšmės kibernetinio incidento vertinimo ataskaitoje turi būti nurodyta žinoma informacija:

13.1. VLII komponentas, kuriame nustatytas pažeidimas (informacinė sistema, elektroninių ryšių tinklas, tarnybinė stotis ir panašiai);

13.2. kibernetinio incidento veikimo trukmė;

13.3. kibernetinio incidento šaltinis;

13.4. kibernetinio incidento požymiai;

13.5. kibernetinio incidento veikimo metodas;

13.6. galimos kibernetinio incidento pasekmės;

13.7. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

13.8. kibernetinio incidento būsena (aktyvus, pasyvus);

13.9. priemonės, kuriomis kibernetinis incidentas nustatytas;

13.10. galimos kibernetinio incidento valdymo priemonės.

14. VLII administratorius bei kiti specialistai, įtraukti į Atkūrimo grupę, atkuria VLII veiklą, nustato ir pašalina elektroninės informacijos saugos (kibernetinio saugumo) incidento atsiradimo priežastis, likviduoja padarinius, padedant VLII naudotojams nustato ar tenkinami VLII veiklos atkūrimo kriterijai, apie darbų eigą ir pabaigą informuoja VLII saugos įgaliotinį (kibernetinio saugumo vadovą).

15. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) visą elektroninės informacijos saugos (kibernetinio saugumo) incidento tyrimo ir valdymo metu surinktą informaciją teikia Valdymo ir atkūrimo grupės vadovui;

16. VLII saugos įgaliotinis (kibernetinio saugumo vadovas) apie didelės ir vidutinės reikšmės kibernetinio incidento sustabdymą ir pašalinimą Centrui praneša ne vėliau kaip per 2 valandas nuo elektroninės informacijos saugos (kibernetinio saugumo) sustabdymo ir pašalinimo;

17. apie kibernetinius incidentus Centras turi būti informuojamas naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės – Centro nurodytais kontaktais.

Viešosios įstaigos Vilkpėdės ligoninės
informacinių išteklių veiklos tęstinumo
valdymo plano
2 priedas

(Viešosios įstaigos Vilkpėdės ligoninės informacinių išteklių elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

VIEŠOSIOS ĮSTAIGOS VILKPĖDĖS LIGONINĖS INFORMACINIŲ IŠTEKLIŲ ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20__m. _____d.

Nr.	Elektroninės informacijos saugos incidentas					
	Požymio kodas	**Įvykio aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Pašalino (vardas, pavardė)**	**VLII saugos įgaliotinis (kibernetinio saugumo vadovas) (vardas, pavardė, parašas)**
1.						
2.						
3.						
4.						
5.						
6.						

Elektroninės informacijos saugos incidento požymiai:
1. Patalpų pažeidimas arba praradimas.
2. Elektros tiekimo sutrikimai.
3. Ryšio sutrikimai.
4. Tarnybinių stočių sugadinimas ir (arba) praradimas.
5. Programinės įrangos sugadinimas.
6. Duomenų sugadinimas, praradimas arba atskleidimas.

Viešosios įstaigos Vilkpėdės ligoninės
informacinių išteklių veiklos tęstinumo
valdymo plano
3 priedas

VLII VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Nenumatytos situacijos rūšis	Veiksmai esant nenumatytai situacijai	Už veiklos atkūrimo veiksmus atsakingi asmenys
1. Patalpų pažeidimas arba praradimas	1.1. personalo evakuacija;	Valdymo ir atkūrimo grupės vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
	1.2. avarinių tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
	1.3. žalos įvertinimas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
	1.4. esant reikalui, darbo organizavimas atsarginėse patalpose;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	1.5. pažeistų ryšio linijų ir sugadintos techninės įrangos atstatymo ir duomenų atkūrimo organizavimas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	1.6. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
2. Elektros tiekimo sutrikimai	2.1. elektros tiekimo sutrikimo masto ir kritiškumo įvertinimas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	2.2. kreipimasis į elektros energijos tiekimo bendrovę dėl sutrikimo pašalinimo trukmės prognozės;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	2.3. vietinio elektros tinklo atstatymo organizavimas, jei buvo pažeistas informacinių išteklių veiklą užtikrinantis elektros tinklas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	2.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
3. Ryšio sutrikimai	3.1. kritiškumo įvertinimas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)

Nenumatytos situacijos rūšis	Veiksmai esant nenumatytai situacijai	Už veiklos atkūrimo veiksmus atsakingi asmenys
	3.2. ryšio sutrikimo priežasties nustatymas;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	3.3. kreipimasis į ryšio paslaugų tiekėją dėl sutrikimo pašalinimo trukmės prognozės;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
	3.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
4. Tarnybinių stočių sugadinimas ir (arba) praradimas	4.1. kritiškumo įvertinimas	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	4.2. vagystės arba vandalizmo atvejais teisėsaugos tarnybų informavimas ir jų nurodymų vykdymas	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
	4.3. esamų techninės įrangos išteklių perskirstymas, siekiant kompensuoti praradimą;	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	4.4. iškilus reikalui, kreipimasis į techninės įrangos tiekėjus dėl sugadintos įrangos remonto ar dėl naujos techninės įrangos įsigijimo;	VLII administratorius
	4.5. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
5. Programinės įrangos sugadinimas	5.1. kritiškumo įvertinimas	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	5.2. sugadintos programinės įrangos atstatymas iš kopijų	VLII administratorius
	5.3. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)
6. Duomenų sugadinimas, praradimas arba atskleidimas	6.1. kritiškumo įvertinimas	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius
	6.2. neteisėto duomenų sugadinimo arba atskleidimo atvejais teisėsaugos tarnybų informavimas ir jų nurodymų vykdymas	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas) VLII administratorius

Nenumatytos situacijos rūšis	Veiksmai esant nenumatytai situacijai	Už veiklos atkūrimo veiksmus atsakingi asmenys
	6.3. Informacinių išteklių veiklos sutrikimo dėl duomenų sugadinimo ar praradimo atvejais duomenų atstatymas iš kopijų	VLII administratorius
	6.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje	Valdymo ir atkūrimo vadovas VLII saugos įgaliotinis (kibernetinio saugumo vadovas)

Viešosios įstaigos Vilkpėdės ligoninės
informacinių išteklių veiklos tęstinumo
valdymo plano
4 priedas

KIBERNETINIŲ INCIDENTŲ KATEGORIJŲ SĄRAŠAS

Kibernetinis incidentas		
Grupė	Apibūdinimas	Kategorija
Kenkimo programinė įranga (angl. *Malicious Software*)	Kenkimo programinė įranga, kai darbo ar tarnybinės stotys aktyviai kontroliuojamos įsibrovėlių (pavyzdžiui, užpakalinės durys (angl. *back door*) Modernios kenkimo programinės įrangos (angl. *advanced persistent threat, APT*) aptikimas VLII. Kenkimo programinė įranga, trikdanti VLII kibernetinio saugumo priemonių darbą	D[1]
	Kenkimo programinė įranga, kurios neaptinka VLII darbo stotyje veikianti antivirusinė programinė įranga. VLII veikianti kenkimo programinė įranga, kurią aptinka antivirusinė programinė įranga per reguliarų patikrinimą	V[2]
	VLII laikmenose ar darbo ir tarnybinėse stotyse veikianti kenkimo programinė įranga, kurią iš karto aptinka antivirusinė programinė įranga. Socialinės inžinerijos metodų naudojimas (manipuliavimas VLII naudotojų emocijomis ir psichologija, pastabumo stoka, technologijų neišmanymu), kai bandoma įtikinti VLII naudotoją atlikti grėsmę VLII keliančius veiksmus, tačiau VLII naudotojas atpažįsta grėsmę ir neatlieka kenkimo programinę įrangą aktyvinančių veiksmų	N[3]
Įsilaužimas	Vykdoma vidinė VLII žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita), aptikta VLII (neskaitant kenkimo programinės įrangos), sukėlusi VLII veiklos sutrikimus. Piktybiniai veiksmai prieš VLII kibernetinio saugumo priemones	D
	Vykdoma vidinė VLII žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita), aptikta VLII infrastruktūroje	V
VLII perimetro žvalgyba	Vykdoma aktyvi (slaptažodžių parinkimas, bandymai išnaudoti pažeidžiamumus, kita) VLII perimetro žvalgyba ar įtartina veikla (neskaitant kenksmingos programinės įrangos), mėginama paveikti VLII kibernetinio saugumo priemones	V
	Vykdoma VLII perimetro priemonių žvalgyba (nebandant įsilaužti)	N
VLII trikdymas	Veiksmas, ilgiau nei 4 valandoms sutrikdęs VLII veiklą	D
	Veiksmas, kuriuo trikdoma (angl. *Denial of Service, DoS*) VLII veikla	V
Neteisėta veika	Vagystė, apgavystė ir panašūs kriminalinio pobūdžio kibernetiniai incidentai	V
Vientisumo pažeidimas	VLII jų dalies pažeidimas, sutrikdantis VLII teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomų duomenų ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti VLII naudotojų pasitikėjimą jais	V

[1] Didelės reikšmės kibernetinis incidentas.
[2] Vidutinės reikšmės kibernetinis incidentas.
[3] Nereikšmingas kibernetinis incidentas.

Viešosios įstaigos Vilkpėdės ligoninės
informacinių išteklių veiklos tęstinumo
valdymo plano
5 priedas

VLII VEIKLOS TĘSTINUMO VALDYMO PLANO BANDYMO ATASKAITA

(Grupės susitikimo data)

Veiklos tęstinumo valdymo plano bandyme dalyvavo:
1. _____
2. _____
3. _____
4. _____
5. _____

Elektroninės informacijos saugos (kibernetinio saugumo) incidento scenarijus:

VLII elementas, kurį paveikė elektroninės informacijos saugos (kibernetinio saugumo) incidentas:

Elektroninės informacijos saugos (kibernetinio saugumo) incidento šalinimo eiga:

Rasti VLII veiklos tęstinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti VLII veiklos tęstinumo valdymo planą:

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)