PATVIRTINTA

 Viešosios įstaigos Vilniaus miesto

 klinikinės ligoninės direktoriaus

 2022 m. balandžio 15 d. įsakymu Nr.V1-114/22(1.1)

**VMKL INFORMACINĖS SISTEMOS**

**VEIKLOS TĘSTINUMO VALDYMO PLANAS**

**I SKYRIUS**

**Bendrosios nuostatos**

1. Viešosios įstaigos Vilniaus miesto klinikinė ligoninė (toliau – VMKL) valdomos ir tvarkomos informacinės sistemos (toliau – IS) veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja VMKL IS veiklos tęstinumo užtikrinimą.

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

3. Planas parengtas pagrindinio IS tvarkytojo (toliau – tvarkytojas) patalpoms, esančioms Antakalnio g. 57, LT-10207 Vilnius, kuriose yra pagrindinė IS informacinių technologijų infrastruktūra, reikalinga IS veiklai. IS komponentų, kurie yra IS kitų tvarkytojų (toliau – tvarkytojai) organizacijose, veiklos tęstinumo valdymą ir veiklos atkūrimą reglamentuoja IS kitų tvarkytojų veiklos tęstinumo valdymą reglamentuojantys dokumentai.

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

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

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

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

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

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

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

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

8.1.3. koordinuoti kibernetinių ir elektroninės informacijos saugos incidentų tyrimą;

8.2. IS administratorius (toliau – administratorius) turi:

8.2.1. dalyvauti atliekant Plano 17 punkte nurodytas funkcijas;

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

8.3. IS naudotojai vykdo Veiklos tęstinumo valdymo grupės nurodymus.

9. Asmenys, atsakingi už kibernetinių incidentų tyrimą ir pranešimą apie kibernetinius incidentus kompetentingoms institucijoms nurodyti 1 priedo 1 lentelėje.

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

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

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

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

12.2. IS elektroninė informacija nuolat atnaujinama ir išsaugoma;

12.3. užtikrintas IS elektroninės informacijos vientisumas ir konfidencialumas;

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

12.5. užtikrintas IS prieinamumas – ne mažiau kaip 95 proc. laiko visą parą (IS neprieinamumo bendra trukmė per metus valandomis – iki 438 val.).

**II SKYRIUS**

**Organizacinės nuostatos**

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

14. Veiklos tęstinumo valdymo grupės sudėtis:

14.1. Veiklos tęstinumo valdymo grupės vadovas: VMKL direktorius;

14.2. Veiklos tęstinumo valdymo grupės vadovo pavaduotojas: VMKL IS saugos įgaliotinis;

14.3. Veiklos tęstinumo valdymo grupės nariai:

14.3.1. VMKL Duomenų apsaugos pareigūnas;

14.3.1. VMKL IS administratorius;

14.3.2. VMKL Informacinių technologijų ir komunikacijų skyriaus vedėjas;

14.3.3. VMKL Ryšių su visuomene specialistas;

14.3.4. VMKL Teisės ir bendrųjų reikalų skyriaus teisininkas;

14.3.5. VMKL Vyriausiasis finansininkas;

14.3.6. VMKL Inžinerinio skyriaus vedėjas.

14.3.7. VMKL Ūkio skyriaus vedėjas.

15. Veiklos tęstinumo valdymo grupės funkcijos:

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

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

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

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

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

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

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

16. Veiklos atkūrimo grupės sudėtis:

16.1. Veiklos atkūrimo grupės vadovas: VMKL IS saugos įgaliotinis;

16.2. Veiklos atkūrimo grupės vadovo pavaduotojas: VMKL IS administratorius;

16.3. Veiklos atkūrimo grupės nariai:

16.3.1. VMKL Informacinių technologijų ir komunikacijų skyriaus vedėjas;

16.3.2. VMKL Informacinių technologijų ir komunikacijų skyriaus kompiuterinių sistemų administratorius.

16.3.4. IS išorės administratorius.

17. Veiklos atkūrimo grupės funkcijos:

17.1. tarnybinių stočių veikimo atkūrimo organizavimas;

17.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

17.3. IS elektroninės informacijos atkūrimo organizavimas;

17.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

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

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

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

20.1. turi atitikti priešgaisrinės saugos reikalavimus;

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

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

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

20.5. turi būti atskirtos nuo bendrojo naudojimo patalpų;

20.6. turi būti interneto ryšio prieiga;

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

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

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

21. Atsarginės patalpos, pritaikytos IS atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, yra Antakalnio g. 57, LT-10207 Vilnius, Vaikų korpuse. Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė organizuoja bendrą susirinkimą, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, nenumatytoms situacijoms arba įvykus esminiams organizaciniams IS ar jų komponentų pokyčiams.

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

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

**III SKYRIUS**

**Aprašomosios nuostatos**

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

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

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

24.2.1. tarnybinės stotys;

24.2.2. kompiuterių tinklo ir telefonų tinklo mazgai;

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

24.2.4. elektros įvedimo pastate vietos;

24.2.5. IS kompiuterių tinklo fizinio ir loginio sujungimo schemos.

24.3. kompiuterinės, techninės ir programinės įrangos sutarčių sąrašas;

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

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

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

24.7. elektroninės informacijos teikimo sutarčių sąrašas.

25. Už Plano 24.1.–24.6. papunkčiuose nurodytų dokumentų parengimo organizavimą, saugojimą, nuolatinį atnaujinimą ir kompiuterinės, techninės ir programinės įrangos sutarčių vykdymo priežiūrą atsakingas VMKL IS administratorius. Šiame punkte nurodyti dokumentai saugomi išspausdinti VMKL Informacinių technologijų ir komunikacijos skyriuje. Jeigu naudojama IS įranga (pagal nuomos, panaudos ar kitas sutartis) priklauso trečiajai šaliai ir yra jos patalpose, sutarties su trečiąja šalimi kopija turi būti saugoma kartu su šiame punkte nurodytais dokumentais.

26. Už Plano 24.7. papunktyje nurodyto dokumento parengimą, saugojimą, nuolatinį atnaujinimą ir elektroninės informacijos teikimo sutarčių vykdymo priežiūrą pagal kompetenciją atsakingas VMKL Teisės ir bendrųjų reikalų skyriaus teisininkas. Elektroninės informacijos teikimo sutarčių sąrašas saugomas išspausdintas VMKL Teisės ir bendrųjų reikalų skyriuje.

**IV SKYRIUS**

**Plano veiksmingumo išbandymo nuostatos**

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

28. Plano veiksmingumo išbandymo rezultatai turi būti naudojami Planui atnaujinti. Nustačius Plano veiksmingumo trūkumų, rengiama pastebėtų Plano veiksmingumo trūkumų šalinimo ataskaita. Už Plano veiksmingumo trūkumų šalinimo ataskaitos parengimą ir pateikimą IS valdytojui atsakingas VMKL saugos įgaliotinis. Plano veiksmingumo trūkumų šalinimo ataskaita ne vėliau kaip per penkias darbo dienas nuo šio dokumento priėmimo pateikiama Nacionaliniam kibernetinio saugumo centrui.

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

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

30.1. IS neprieinamumas valandomis per metus;

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

VšĮ Vilniaus miesto klinikinė ligoninė informacinės sistemos veiklos tęstinumo valdymo plano

priedas

**VMKL LIGONINĖS INFORMACINĖS SISTEMOS**

**veiklos ATKŪRIMO DETALUSIS PLANAS**

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

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

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

3.1. tarnybinių stočių veikimo atkūrimas:

3.1.1. duomenų bazės veikimo atkūrimas;

3.1.2. taikomųjų programų veikimo atkūrimas;

3.2. kompiuterių tinklo veikimo atkūrimas;

3.3. elektroninės informacijos atkūrimas;

3.4. taikomųjų programų veikimo atkūrimas;

3.5. interneto ryšio atkūrimas;

3.6. pagrindinio IS tvarkytojo kompiuterinių darbo vietų veikimo atkūrimas;

3.7. kitų IS tvarkytojų kompiuterinių darbo vietų veikimo atkūrimas.

4. IS veiklos atkūrimo veiksmai, atsižvelgiant į kibernetinio ar elektroninės informacijos saugos incidento tipą ir mastą, veiklos atkūrimo veiksmų pobūdį, turi būti atlikti per kuo trumpesnį terminą, kuris neturi būti ilgesnis kaip 16 valandų. IS veiklos atkūrimo detalūs veiksmai nurodyti 1 lentelėje.

1 lentelė. IS atkūrimo detalūs veiksmai

|  |  |  |  |
| --- | --- | --- | --- |
| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
| 1. Kibernetinis incidentas
 | * 1. Kibernetinio incidento įvertinimas ir priskyrimas pagal 2 lentelės sąrašą, priemonių pavojui sustabdyti ir padarytai žalai likviduoti sudarymas
 | * + 1. Kibernetinio incidento nustatymas
 | VMKL saugos įgaliotinis |
|  |  | * + 1. Pranešti Nacionaliniam kibernetinio saugumo centrui naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionaliniam kibernetinio saugumo centro nurodytais kontaktais, vadovaujantis 3 lentele apie:
* didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;
* vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;;
* nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.
 | VMKL saugos įgaliotinis, VMKL Duomenų apsaugos pareigūnas |
|  |  | * + 1. Priemonių sustabdyti ir padarytai žalai likviduoti sudarymas
 | VMKL saugos įgaliotinis |
|  |  | * + 1. Pranešti Nacionaliniam kibernetinio saugumo centrui, naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionalinio kibernetinio saugumo centro nurodytais kontaktais, vadovaujantis 4 lentele, apie:
* didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;
* vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;;
 | VMKL saugos įgaliotinis, VMKL Duomenų apsaugos pareigūnas |
|  |  | * + 1. Nustačius, kad SPĮ negalės savarankiškai ištirti ar suvaldyti kibernetinio incidento per maksimaliai leistiną paslaugos neveikimo laiką, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo kreiptis pagalbos į Nacionalinį kibernetinio saugumo centrą.
 | VMKL saugos įgaliotinis |
|  | * 1. Veiksmai, Nacionaliniam kibernetinio saugumo centrui perėmus tirti ir (ar) organizuoti pavojingo kibernetinio incidento valdymą
 | * + 1. Rinkti, apdoroti informaciją, susijusią su kibernetiniu incidentu, ir ne rečiau kaip kas keturias valandas ją teikti Nacionaliniam kibernetinio saugumo centrui;
 | VMKL saugos įgaliotinis |
|  |  | * + 1. ne rečiau kaip kas keturias valandas teikti Nacionaliniam kibernetinio saugumo centrui informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus vadovaujantis 4 lentele;
 | VMKL saugos įgaliotinis |
|  |  | * + 1. vykdyti Nacionalinio kibernetinio saugumo centro nurodymus, susijusius su kibernetinio incidento tyrimu ir (ar) valdymo organizavimu, ir dalyvauti kibernetinio incidento valdymo procese, taikant kibernetinio saugumo užtikrinimo priemones.
 | VMKL saugos įgaliotinis |
|  | * 1. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas. Pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas. Kibernetinio incidento pašalinimas
 | * + 1. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas
 | VMKL saugos įgaliotinis |
|  |  | * + 1. Pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas
 | VMKL saugos įgaliotinis |
|  |  | * + 1. Kibernetinio incidento pašalinimas
 | VMKL IS administratorius |
|  |  | * + 1. Pranešti Nacionaliniam kibernetinio saugumo centrui naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės Nacionalinio kibernetinio saugumo centro nurodytais kontaktais, apie didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.
 | VMKL saugos įgaliotinis |
|  |  | * + 1. ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo informuoti teikiamų paslaugų gavėjus (jeigu tokių yra), jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos informacinės sistemos teikiamų paslaugų gavėjui.
 | VMKL saugos įgaliotinis |
|  | * 1. Kibernetinio incidento analizė pabaigus kibernetinių incidentų tyrimą
 | * + 1. ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikti kibernetinio incidento analizės rezultatus Nacionaliniam kibernetinio saugumo centrui ir kibernetinio saugumo informaciniame tinkle paskelbti susistemintą ir aktualią neįslaptintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą;
 | VMKL saugos įgaliotinis |
|  |  | * + 1. imtis priemonių, kad būtų pašalintas ryšių ir informacinės sistemos pažeidžiamumas;
 | VMKL saugos įgaliotinis |
|  |  | * + 1. įvertinti ryšių ir informacinės sistemos riziką ir atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;
 | VMKL saugos įgaliotinis |
|  |  | * + 1. nustačius teisinio reglamentavimo spragų, inicijuoti informacinės sistemos kibernetinį saugumą reglamentuojančius SPĮ teisės aktus.
 | VMKL saugos įgaliotinis |
| 1. Tarnybinės stoties, komutacinės įrangos gedimas ar tyčinis sugadinimas
 | * 1. Pranešti teisėsaugos tarnybai (tyčios atveju), draudimo bendrovei apie įvykį
 | * + 1. Nenumatytos situacijos pasekmę likviduojančių darbuotojų paskyrimas, instruktavimas, jų veiksmų nustatymas
 | VMKL Teisės ir bendrųjų reikalų skyriaus teisininkas |
|  | * 1. Nenumatytos situacijos pasekmės šalinimas
 | * + 1. Kreiptis į įrangos teikėjus dėl įrangos remonto ar naujos įsigijimo
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  |  | * + 1. Įsigytos įrangos paskyrimas
 | VMKL IS administratorius |
| 1. Ryšio sutrikimai
 | * 1. Ryšio sutrikimo priežasčių nustatymas
 | * + 1. Kreiptis į ryšio paslaugų teikėją
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  | * 1. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir šalinimo prognozės
 | * + 1. Nustatyti ir įgyvendinti priemones, kad sutrikimai nesikartotų
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  | * 1. Sutrikimo šalinimas
 | * + 1. Kreiptis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
| 1. Programinės įrangos sugadinimas, praradimas
 | * 1. Nenumatytos situacijos įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas
 | * + 1. Nenumatytos situacijos įvertinimas
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  |  | * + 1. IS programinės įrangos priežiūrą vykdančių rangovų informavimas.
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  |  | * + 1. Priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas
 | Rangovas (-ai), VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  | * 1. Nenumatytos situacijos pasekmę likviduojančių darbuotojų paskyrimas. Žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas
 | * + 1. Žalą likviduojančių darbuotojų instruktavimas
 | VMKL Informacinių technologijų ir komunikacijos skyriaus vedėjas |
|  | * 1. Programinės įrangos kopijų periodinis gaminimas
 | * + 1. Sugadintos ar prarastos programinės įrangos atkūrimo organizavimas
 | VMKL IS administratorius, IS išorės administratorius |
| 1. Energijos tiekimo sutrikimai
 | * 1. Energijos tiekimo sutrikimo priežasčių nustatymas. Tarnybinės stoties, kitos techninės įrangos energijos maitinimo išjungimas
 | * + 1. Sutrikimų pašalinimo organizavimas
 | VMKL Inžinerinio skyriaus vedėjai |
|  | * 1. Kreipimasis į energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių
 | * + 1. Rekomendacijų iš energijos tiekimo tarnybos gavimas
 | VMKL Inžinerinio skyriaus vedėjas |
|  | * 1. Sutrikimų pašalinimas
 | * + 1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas, įgyvendinimas
 | VMKL Inžinerinio skyriaus vedėjas |
|  |  | * + 1. Padarytos žalos įvertinimas
 | VMKL Inžinerinio skyriaus vedėjas |
|  |  | * + 1. Žalą likviduojančių darbuotojų instruktavimas
 | VMKL Inžinerinio skyriaus vedėjas |

2 lentelė. Kibernetinių incidentų sąrašas

| **Eil. Nr.** | **Kibernetinio incidento grupės** | **Kibernetinio incidento poveikis****Kibernetinio****incidento pogrupiai** | **Nereikšmingas (N)**(bent vienas iš kriterijų) | **Vidutinis (V)**(du ar daugiaukriterijų) | **Didelis (D)**(du ar daugiaukriterijų) | **Pavojingas (P)**(bent vienas iškriterijų) |
| --- | --- | --- | --- | --- | --- | --- |
| RIS trikdoma < 1 val. | Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 % | Paslauga teikiama, bet trikdoma | Nuostoliai < 250 000 Eur | RIS trikdoma ≥ 1 val., bet < 2 val. | Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 % | Paslauga trikdoma dalyje šalies teritorijos | Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas | Nuostoliai ≥ 250 000, bet < 500 000 Eur | RIS trikdoma ≥ 2 val. | Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 % | Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje | Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas | Nuostoliai ≥ 500 000 Eur | RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas | Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % | Sutrikdomas (gali sutrikti) paslaugų veikimas visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų sąraše |
| 1.  | Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content*, *spam*) | 1.1. Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ryšių ir informacinės sistemos (toliau – RIS) veiklą ir (ar) teikiamas paslaugas | N | V | D | P |
| 1.2. Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas  | N |  |  |  |
| 2.  | Kenkimo programinė įranga (angl*. malicious software / code*)Programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims | 2.1. Aptikta moderni kenkimo programinė įranga (angl*. advanced persistent threat, APT*) |  | V | D | P |
| 2.2. RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys“ (angl*. back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl*. Botnet*) infrastruktūros dalimi |  | V | D | P |
| 2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą |  | V | D | P |
| 2.4. Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja | N | V |  |  |
| 2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus | N | V | D | P |
| 3.  | Informacijos rinkimas (angl*. information gathering*)Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl*. social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl*. phishing*) arba atlikti norimus veiksmus | 3.1. RIS paketų / informacijos perėmimas |  | V | D | P |
| 3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas) |  | V | D | P |
| 3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti) | N | V |  |  |
| 3.4. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją | N | V |  |  |
| 4.  | Mėginimas įsilaužti (angl*. intrusion attempts*)Mėginimas įsilaužti arba sutrikdyti RIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack* *signature*) | 4.1. Išnaudojamas vienas ar keli nežinomi (angl*. zero day*) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią RIS |  | V | D | P |
| 4.2. Išnaudojamas vienas ar keli nežinomi (angl*. zero day*) pažeidžiamumai | N | V | D | P |
| 4.3. Vidinė RIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita) |  | V | D | P |
| 4.4. Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisijungti prie RIS parenkant slaptažodžius | N | V |  |  |
| 5.  | Įsilaužimas (angl*. intrusions*)Sėkmingas įsilaužimas ir (ar) neteisėtas RIS, taikomosios programinės įrangos ar paslaugos naudojimas (angl*. privileged account compromise, unprivileged account compromise, application compromise*) | 5.1. Veiksmai prieš RIS ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, RIS ar jos dalies pažeidimas, sutrikdantis RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS naudotojų pasitikėjimą jais |  | V | D | P |
|
| 5.2. Gaunama neteisėta prieiga prie RIS, taikomosios programinės įrangos ar paslaugos |  | V | D | P |
| 6.  | Paslaugų trikdymas, prieinamumo pažeidimai (angl*. availability*)Veiksmai, kuriais trikdoma RIS veikla, teikiamos paslaugos (angl*. DoS, DDoS*), RIS ar jos dalies pažeidimas, sutrikdantis RIS ir (ar) jos teikiamas paslaugas (angl*. sabotage, outage*) | 6.1. Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas |  | V | D | P |
| 6.2. Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui | N | V |  |  |
| 6.3. Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui | N | V |  |  |
| 7.  | Informacijos turinio saugumo pažeidimai (angl*. information content security*)Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas (angl*. unauthorised access to information, unauthorised modification of information*) | 7.1. Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai ir (ar) teikiamoms paslaugoms |  | V | D | P |
| 7.2. Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas | N | V | D | P |
| 8.  | Neteisėta veikla, sukčiavimas (angl*. fraud*)Vagystė, apgavystė, neteisėtas išteklių (angl*. unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl*. copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai | 8.1. Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms | N | V | D | P |
| 9.  | KitaIncidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų | N | V | D | P |

|  |
| --- |
| **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 MML IS.Kenkimo programinė įranga, trikdanti MML IS kibernetinio saugumo priemonių darbą. | D1 |
| Kenkimo programinė įranga, kurios neaptinka MML IS darbo stotyje veikianti antivirusinė programinė įranga.MML IS veikianti kenkimo programinė įranga, kurią aptinka antivirusinė programinė įranga per reguliarų patikrinimą. | V2 |
| MML IS laikmenose ar darbo ir tarnybinėse stotyse veikianti kenkimo programinė įranga, kurią iš karto aptinka antivirusinė programinė įranga.Socialinės inžinerijos metodų naudojimas (manipuliavimas MML IS naudotojų emocijomis ir psichologija, pastabumo stoka, technologijų neišmanymu), kai bandoma įtikinti MML IS naudotoją atlikti grėsmę MML IS keliančius veiksmus, tačiau MML IS naudotojas atpažįsta grėsmę ir neatlieka kenkimo programinę įrangą aktyvinančių veiksmų. | N3 |
| Įsilaužimas | Vykdoma vidinė MML IS žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita) aptikta MML IS (neskaitant kenkimo programinės įrangos), sukėlusi MML IS veiklos sutrikimus.Piktybiniai veiksmai prieš MML IS kibernetinio saugumo priemones | D |
| Vykdoma vidinė MML IS žvalgyba ar kita įtartina veikla (prievadų skenavimas, slaptažodžių parinkimas, kita), aptikta MML IS infrastruktūroje | V |
| MML IS perimetro žvalgyba | Vykdoma aktyvi (slaptažodžių parinkimas, bandymai išnaudoti pažeidžiamumus, kita) MML IS perimetro žvalgyba ar įtartina veikla (neskaitant kenksmingos programinės įrangos), mėginama paveikti MML IS kibernetinio saugumo priemones | V |
| Vykdoma MML IS perimetro priemonių žvalgyba (nebandant įsilaužti) | N |
| MML IS | Veiksmas, ilgiau nei 4 valandoms sutrikdęs MML IS veiklą. | D |
| Veiksmas, kuriuo trikdoma (angl. *Denial of Service, DoS*) MML IS | V |
| Neteisėta veikla | Vagystė, apgavystė ir panašūs kriminalinio pobūdžio kibernetiniai incidentai | V |
| Vientisumo pažeidimas | MML IS ar jos dalies pažeidimas, sutrikdantis MML IS teikiamų paslaugų nepertraukiamą tiekimą, galintis turėti įtakos tvarkomų duomenų ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti MML IS naudotojų pasitikėjimą jais. | V |

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

3 lentelė. Pranešimas apie įvykusį kibernetinį incidentą.

|  |  |
| --- | --- |
|  | Aprašymas |
| Kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal 2 lentelėje pateiktus kriterijus |  |
| Trumpas kibernetinio incidento apibūdinimas |  |
| Tikslus laikas, kada kibernetinis incidentas įvyko ir nustatytas |  |
| Kibernetinio incidento šalinimo tvarka (turi būti nurodyta, ar tai prioritetas, ar ne) |  |
| Tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita. |  |

4 lentelė. Kibernetinio incidento tyrimo ataskaita.

|  |  |
| --- | --- |
|  | Aprašymas |
| Kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal 2 lentelėje pateiktus kriterijus |  |
| Ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema, tarnybinė stotis ir panašiai) | Viešosios įstaigos Vilniaus miesto klinikinės ligoninės ir Viešosios įstaigos Respublikinės Vilniaus psichiatrijos ligoninės informacinė sistema |
| Kibernetinio incidento veikimo trukmė |  |
| Kibernetinio incidento šaltinis |  |
| Kibernetinio incidento požymiai |  |
| Kibernetinio incidento veikimo metodas |  |
| Galimos ir (ar) nustatytos kibernetinio incidento pasekmės |  |
| Kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas |  |
| Kibernetinio incidento būsena (aktyvus, pasyvus) |  |
| Priemonės, kuriomis kibernetinis incidentas nustatytas |  |
| Galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės |  |
| Tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_