PATVIRTINTA
Lietuvos dailės muziejaus direktoriaus
2019 m. spalio 25 d. įsakymu Nr. V.1-137

# LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (toliau – informacinė sistema) veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja informacinės sistemos veiklos tęstinumo užtikrinimą.
2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose 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“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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“, Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas), Lietuvos integralios muziejų informacinės sistemos duomenų saugos nuostatuose ir kituose teisės aktuose bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose.
3. Planas įsigalioja įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, dėl kurio informacinės sistemos tvarkytojas negali teikti viešųjų ir administracinių paslaugų visiems informacinės sistemos naudotojams arba daliai jų ir būtina atkurti įprastą informacinės sistemos veiklą informacinės sistemos valdytojo ar tvarkytojų patalpose arba atsarginėse patalpose.
4. Plano nuostatos taip pat taikomos informacinės sistemos veiklai atkurti po stichinės nelaimės, avarijos ar kitų ekstremalių situacijų.
5. Kibernetinių ir elektroninės informacijos saugos incidentų tyrimas atliekamas vadovaujantis Planu ir Nacionaliniu kibernetinių incidentų valdymo planu.
6. Informacinės sistemos saugos įgaliotinio (toliau – saugos įgaliotinis), informacinės sistemos kibernetinio saugumo vadovo (toliau – kibernetinio saugumo vadovas), informacinės sistemos administratoriaus (toliau – administratorius), informacinės sistemos lokalios tarnybinės stoties

administratorių (toliau – LIMIS-M administratoriai), naudotojų ir kitų asmenų veiksmai nustatyti šio Plano priede.

7. Įvykus kibernetiniam ar elektroninės informacijos saugos incidentui atsakingi asmenys atlieka šiuos veiksmus:
   7.1. naudotojai vykdo veiklos tęstinumo valdymo grupės nurodymus;
   7.2. administratorius ir LIMIS-M administratoriai, kai incidentas įvyksta informacinės sistemos lokalioje tarnybinėje stotyje:
      7.2.1. nedelsdamas turi imtis veiksmų, reikalingų saugos incidentui stabdyti, padariniams likviduoti, ir apie tai pranešti saugos įgaliotiniui ar kibernetinio saugumo vadovui;
      7.2.2. nagrinėja saugos incidentą;
      7.2.3. suderinęs su saugos įgaliotiniu, atlieka neatidėliotinus administravimo veiksmus, skirtus saugos incidento plėtrai sustabdyti ir jo tyrimui būtinai informacijai surinkti;
      7.2.4. surenka visą su saugos incidentu susijusią informaciją ir aprašo incidentą, nurodydamas incidento vietą, laiką, pobūdį, informacinės sistemos atkuriamuosius darbus ir kitą su saugos incidentu susijusią informaciją;
      7.2.5. dalyvauja veiklos tęstinumo valdymo grupei ir veiklos atkūrimo grupei atliekant Plane nurodytas funkcijas;
      7.2.6. vykdo kitus Plane ir jo priede nurodytus veiksmus ir veiklos tęstinumo valdymo grupės ar veiklos atkūrimo grupės pavestas užduotis;
   7.3. saugos įgaliotinis, kibernetinio saugumo vadovas:
      7.3.1. gavęs informaciją apie saugos incidentą įvertins saugos incidento reikšmingumą bei apie incidentą informuoja veiklos tęstinumo valdymo grupės vadovą;
      7.3.2. pagal savo įgaliojimus bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, kibernetinius ir elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su kibernetiniais ir elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka sudarytos elektroninės informacijos saugos ir kibernetinio saugumo darbo grupės;
      7.3.3. pagal savo įgaliojimus duoda privalomus vykdyti nurodymus ir pavedimus informacinės sistemos valdytojo ir informacinės sistemos tvarkytojo darbuotojams, jeigu tai būtina elektroninės informacijos saugos ir kibernetinio saugumo politikai įgyvendinti;
      7.3.4. pagal savo įgaliojimus koordinuoja kibernetinių ir elektroninės informacijos saugos incidentų tyrimą;
   7.4. informacinės sistemos valdytojas:
      7.4.1. organizuoja informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – veiklos tęstinumo valdymo grupė) ir informacinės sistemos veiklos atkūrimo grupės (toliau – veiklos atkūrimo grupė) darbą;
      7.4.2. atkuria informacinės sistemos veiklą;
      7.4.3. analizuoja kibernetinių ir elektroninės informacijos saugos incidentų priežastis ir aplinkybes;
      7.4.4. turi teisę naudoti rezervinius finansinius ir kitokius išteklius informacinės sistemos veiklai atkurti.
8. Valdymo grupės vadovas, atsižvelgdamas į saugos incidento pobūdį, gali inicijuoti jo išsamų tyrimą. Nusprendęs pradėti saugos incidento tyrimą, valdymo grupės vadovas teikia informacinės sistemos valdytojo vadovui siūlymą sudaryti atskirą tyrimo komisiją, kuri per penkiolika darbo dienų turi:

8.1. ištirti saugos incidento atsiradimo priežastis;
8.2. nustatyti asmenis, dėl kurių veiksmų ir (ar) neveikimo įvyko saugos incidentas;
8.3. nustatyti saugos incidento pasekmes ar dėl jo atsiradusią žalą;
8.4. parengti ir pateikti valdymo grupės vadovui tyrimo išvadas.

9. Valdymo grupės vadovas, atsižvelgdamas į tyrimo komisijos pateiktas išvadas, turi teisę teikti informacinės sistemos valdytojo vadovui siūlymus dėl atsakomybės taikymo teisės aktų nustatyta tvarka.
10. Plano privalo laikytis informacinės sistemos valdytojas, tvarkytojai, saugos įgaliotinis, kibernetinio saugumo vadovas, duomenų valdymo įgaliotinis, administratoriai, LIMIS-M administratoriai, naudotojai, informacinės sistemos techninės ir programinės įrangos priežiūros paslaugas teikiantys paslaugų teikėjai, jei tokios funkcijos paslaugų teikėjams perduotos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka.
11. Planas pagrįstas šiais pagrindiniais principais:
11.1. informacinės sistemos naudotojų gyvybės ir sveikatos apsauga (būtina užtikrinti visų naudotojų gyvybės ir sveikatos apsaugą ir saugumą, kol trunka kibernetinis ar elektroninės informacijos saugos incidentas ir likviduojami jo padariniai);
11.2. informacinės sistemos veiklos atkūrimas per 12 val.;
11.3. naudotojų mokymas. Naudotojai supažindinami su Planu ir teisės aktais, nustatančiais kiekvieno naudotojo atsakomybę;
11.4. reguliarus Plano veiksmingumo išbandymas. Plano veiksmingumas reguliariai išbandomas teorinių ir (ar) praktinių mokymų metu, modeliuojant kibernetinį ar elektroninės informacijos saugos incidentą. Atsižvelgiant į gautus rezultatus, Planas tikslinamas.
12. Įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, informacinės sistemos veiklai atkurti naudojami rezerviniai informacinės sistemos valdytojo finansiniai ir kitokie ištekliai.
13. Informacinės sistemos veiklos kriterijai, pagal kuriuos nustatoma, ar informacinės sistemos veikla atkurta:
13.1. informacinė sistema priima elektroninę informaciją iš elektroninės informacijos teikėjų;
13.2. informacinės sistemos elektroninė informacija (toliau – elektroninė informacija) nuolat atnaujinama ir išsaugoma;
13.3. užtikrintas elektroninės informacijos vientisumas ir konfidencialumas;
13.4. elektroninė informacija nuolat teikiama naudotojams, susijusiems registrams ir kitoms informacinėms sistemoms;
13.5. užtikrintas informacinės sistemos prieinamumas – per metus ne mažiau kaip 96 proc. viso paros laiko.

## II SKYRIUS
## ORGANIZACINĖS NUOSTATOS

14. Informacinės sistemos veiklos tęstinumui užtikrinti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui sudaroma veiklos tęstinumo valdymo grupė ir veiklos atkūrimo grupė.
15. Veiklos tęstinumo valdymo grupės sudėtis:
15.1. veiklos tęstinumo valdymo grupės vadovas – informacinės sistemos saugos įgaliotinis;

15.2. veiklos tęstinumo valdymo grupės vadovo pavaduotojai: Lietuvos dailės muziejaus filialo Lietuvos muziejų informacijos, skaitmeninimo ir informacinės sistemos centro (toliau – LM ISC LIMIS) vedėjas, Lietuvos dailės muziejaus (toliau – LDM) direktoriaus pavaduotojas strateginiam planavimui, plėtrai ir vadybai;

15.3. veiklos tęstinumo valdymo grupės nariai:

15.3.1. LDM direktoriaus pavaduotojas ūkui;

15.3.2. LDM vyriausioji finansininkė;

15.3.3. LDM Personalo skyriaus vedėjas;

15.3.4. administratorius;

15.3.5. LDM Informacinių sistemų tarnybos vedėjas.

16. Veiklos tęstinumo valdymo grupės funkcijos:

16.1. situacijos analizė ir sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas;

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

16.3. bendravimas su susijusių registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

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

16.5. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, naudojimo kontrolė;

16.6. elektroninės informacijos fizinės saugos organizavimas, įvykus elektroninės informacijos saugos incidentui ar nenumatytai situacijai;

16.7. logistika (asmenų, daiktų, įrangos gabenimo organizavimas);

16.8. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas.

17. Veiklos atkūrimo grupės sudėtis:

17.1. veiklos atkūrimo grupės vadovas – LM ISC LIMIS vedėjas;

17.2. veiklos atkūrimo grupės vadovo pavaduotojai: informacinės sistemos saugos įgaliotinis, administratorius;

17.3. veiklos atkūrimo grupės nariai: LDM Pastatų ir techninių įrenginių eksploatavimo tarnybos vedėjas ir inžinierius, LDM Informacinių sistemų tarnybos vedėjas ir inžinierius, LDM pastatų ir technologinių įrenginių eksploatavimo tarnybos vyr. inžinierius, specialistas atsakingas už LIMIS klasifikavimo sistemos turinį.

18. Veiklos atkūrimo grupės funkcijos:

18.1. tarnybinių stočių veikimo atkūrimo organizavimas;

18.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

18.3. elektroninės informacijos atkūrimo organizavimas;

18.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

19. Personalinę veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės sudėtį tvirtina informacinės sistemos valdytojo vadovas.

20. Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės veiklą organizuoja ir koordinuoja šių grupių vadovai.

21. Informacinės sistemos veiklos atkūrimo detalusis planas pateikiamas Plano priede.

22. Atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, keliami šie reikalavimai:
    22.1. atsarginės patalpos turi atitikti priešgaisrinės saugos reikalavimus;
    22.2. atsarginės patalpos turi atitikti informacinės sistemos techninės įrangos gamintojų nustatytus reikalavimus įrangos darbo aplinkai (pvz., tinkama oro temperatūra, oro drėgmė ir kt.);
    22.3. atsarginėse patalpose turi būti įrengtos langų, durų, informacinės sistemos techninės įrangos, kabelių fizinės apsaugos priemonės;
    22.4. atsarginėse patalpose turi būti įrengta patalpų apsaugos signalizacija, kurios signalai persiunčiami patalpas saugančiai saugos tarnybai;
    22.5. atsarginės patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;
    22.6. atsarginėse patalpose turi būti internetinio ryšio prieiga;
    22.7. atsarginėse patalpose turi būti įrengti nenutrūkstamą elektros tiekimą užtikrinantys maitinimo šaltiniai;
    22.8. atsarginėse patalpose turi būti užtikrintas tinklais perduodamos elektroninės informacijos vientisumas ir konfidencialumas;
    22.9. atsarginėse patalpose turi būti įdiegtos kitos priemonės, atitinkančios antrosios kategorijų informacinės sistemos veiklai ir jų saugumui užtikrinti keliamus reikalavimus.
23. Atsarginės patalpos, pritaikytos informacinės sistemos veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, yra LDM administracijos pastate, adresu Chodkevičių rūmų komplekso rytinis korpusas, Didžioji g. 4, LT-01128 Vilnius.
24. Veiklos tęstinumo valdymo grupė ir veiklos atkūrimo grupė įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, nenumatytoms situacijoms arba įvykus esminiams organizaciniams informacinės sistemos ar jos komponentų pokyčiams organizuoja bendrą susirinkimą.
25. Veiklos tęstinumo valdymo grupė, atlikusi situacijos analizę, informuoja veiklos atkūrimo grupę apie priimtus sprendimus informacinės sistemos veiklos tęstinumo valdymo klausimais. Veiklos atkūrimo grupė, atsižvelgdama į veiklos tęstinumo valdymo grupės priimtus sprendimus, organizuoja informacinės sistemos veiklos atkūrimą.
26. Komunikavimas veiklos tęstinumo valdymo ir veiklos atkūrimo grupėse ir tarp jų vyksta žodžiu ir raštu, keičiantis informacija telefonu ir elektroniniu paštu.

## III SKYRIUS
## APRAŠOMOSIOS NUOSTATOS

27. Informacinės sistemos veiklos tęstinumui užtikrinti turi būti parengti ir saugomi šie dokumentai:
    27.1. informacinės sistemos dokumentacija, kurioje nurodyta informacinės sistemos informacinių technologijų įranga ir jos parametrai;
    27.2. kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukštų patalpų brėžiniai, kuriuose pažymėta:
        27.2.1. tarnybinės stotys;
        27.2.2. kompiuterių tinklo ir telefonų tinklo mazgai;
        27.2.3. kompiuterių tinklo ir telefonų tinklo vedimo tarp pastato aukštų vietos;
        27.2.4. elektros įvedimo pastate vietos;
    27.3. dokumentas, kuriame nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemos;

27.4. dokumentas, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigas;

27.5. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

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

27.7. minimalių funkcinių galimybių informacinių technologijų įrangos, tinkamos informacinės sistemos valdytojo ir tvarkytojo poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui ar nenumatytai situacijai, specifikacija; už šios įrangos priežiūrą atsakingų administratorių sąrašas ir dokumentas, kuriame nurodomi minimalūs reikiamos kompetencijos ar žinių lygio reikalavimai informacinės sistemos veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą;

27.8. elektroninės informacijos teikimo sutarčių sąrašas.

28. Už Plano 27.1–27.7 papunkčiuose nurodytų dokumentų parengimą, saugojimą, nuolatinį atnaujinimą ir kompiuterinės, techninės ir programinės įrangos sutarčių vykdymo priežiūrą atsakingas saugos įgaliotinis. Minėti dokumentai saugomi saugos įgaliotinio darbo vietoje ir administratoriaus darbo vietoje esančiame seife. Jeigu naudojama informacinės sistemos įranga (pagal nuomos, panaudos ar kitas sutartis) priklauso ir yra trečiosios šalies patalpose, sutarties su trečiąja šalimi kopija turi būti saugoma kartu su minėtais dokumentais.

29. Už Plano 27.8 papunktyje nurodyto dokumento parengimą, saugojimą, nuolatinį atnaujinimą ir elektroninės informacijos teikimo sutarčių vykdymo priežiūrą pagal kompetenciją atsakingas LIMIS duomenų valdymo įgaliotinis. Elektroninės informacijos teikimo sutarčių sąrašas saugomas išspausdintas LIMIS duomenų valdymo įgaliotinio darbo vietoje ir administratoriaus darbo vietoje esančiame seife.

## IV SKYRIUS
## PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

30. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus kibernetinio ar elektroninės informacijos saugos incidento ar nenumatytos situacijos simuliacijos metu. Plano veiksmingumo išbandymą organizuoja saugos įgaliotinis.

31. Kibernetinio ar elektroninės informacijos saugos incidento simuliacijos metu gauti rezultatai turi būti naudojami Planui atnaujinti. Nustačius Plano veiksmingumo trūkumų, rengiama pastebėtų trūkumų šalinimo ataskaita. Už Plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą informacinės sistemos valdytojui yra atsakingas saugos įgaliotinis.

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

33. Plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos kopijos ne vėliau kaip per penkias darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

34. Veiklos tęstinumo valdymo procesams tobulinti turi būti matuojami ir vertinami šie rodikliai:

34.1. informacinės sistemos neprieinamumas valandomis per metus;

34.2. informacinės sistemos veiklos atkūrimo, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui ar nenumatytai situacijai, trukmė.

_____

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie
Krašto apsaugos ministerijos
2019 m. spalio 21 d. raštu Nr. (4.2)6K-678

Lietuvos integralios muziejų informacinės sistemos
veiklos tęstinumo valdymo plano priedas

# LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (toliau – informacinė sistema) veiklos atkūrimo detalusis planas (toliau – Atkūrimo planas) reglamentuoja informacinės sistemos atkūrimo veiksmų vykdymo eiliškumą ir atsakingus vykdytojus.
2. Įsigaliojus Atkūrimo planui informacinės sistemos veiklos tęstinumo valdymo grupė (toliau – veiklos tęstinumo valdymo grupė) informuoja informacinės sistemos naudotojus, susijusių registrų ir kitų informacinių sistemų tvarkytojus, kitus suinteresuotus asmenis apie informacinės sistemos veikimo sutrikimus. Informacija teikiama informacinės sistemos viešoje interneto svetainėje ar kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir pan.).
3. Informacinės sistemos veiklos atkūrimo grupė (toliau – veiklos atkūrimo grupė) informacinės sistemos veiklą atkuria pagal šiuos informacinės sistemos funkcijų prioritetus:
   3.1. tarnybinių stočių veikimo atkūrimas:
      3.1.1. duomenų bazių tarnybinių stočių veikimo atkūrimas;
      3.1.2. taikomųjų programų tarnybinių stočių veikimo atkūrimas;
   3.2. kompiuterių tinklo veikimo atkūrimas;
   3.3. informacinės sistemos elektroninės informacijos (toliau – elektroninė informacija) atkūrimas;
   3.4. taikomųjų programų veikimo atkūrimas;
   3.5. interneto ryšio atkūrimas;
   3.6. kompiuterinių darbo vietų veikimo atkūrimas.
4. Informacinės sistemos veiklos atkūrimo veiksmai:

| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
|---|---|---|---|
| 1. Manipuliacija elektronine informacija (pvz., elektroninės informacijos, įskaitant informacinės sistemos programinę įrangą, pakeitimas kita | 1.1. Situacijos analizė | 1.1.1. nustatomas atakos šaltinis, kibernetinio ar elektroninės informacijos saugos incidento padariniai, identifikuojama pakeista, sunaikinta ar kitaip neteisėtai tvarkyta elektroninė informacija;<br>1.1.2. sustabdomas pažeistos elektroninės informacijos teikimas;<br>1.1.3. nustatomos elektroninės informacijos vientisumo pažeidimo, neteisėto tvarkymo priežastys;<br>1.1.4. informuojamos kompetentingos institucijos, kitos suinteresuotos šalys. | Veiklos atkūrimo grupės vadovas |

| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
|---|---|---|---|
| elektronine informacija, elektroninės informacijos iškraipymas, ištrynimas ar kitoks neteisėtas jos naudojimas) | 1.2. Veiksmų plano sudarymas | 1.2.1. sudaromas veiksmų planas manipuliacijos elektronine informacija padariniams likviduoti, informacinės sistemos veiklai atkurti ir informacinei sistemai apsaugoti. | Veiklos tęstinumo valdymo grupės vadovas, veiklos atkūrimo grupės vadovas |
| | 1.3. Padarinių likvidavimas ir veiklos atkūrimas | 1.3.1. imamasi veiksmų neteisėtai veikai sustabdyti;<br>1.3.2. likviduojami kibernetinio ar elektroninės informacijos saugos incidento padariniai, atkuriamas informacinės sistemos veikimas, diegiamos informacinės sistemos apsaugos priemonės;<br>1.3.3. jeigu informacinės sistemos veiklos atkūrimo metu elektroninė informacija atkuriama iš atsarginių kopijų, tikrinama, ar atkurta elektroninė informacija yra teisinga;<br>1.3.4. jeigu nėra galimybės elektroninės informacijos tinkamai atkurti iš atsarginių kopijų, duomenų teikėjų prašoma pateikti elektroninę informaciją iš naujo;<br>1.3.5. atkuriamas elektroninės informacijos paslaugų teikimas;<br>1.3.6. prireikus informacinės sistemos veikla atkuriama atsarginėse patalpose. | Veiklos atkūrimo grupės vadovas |
| 2. Ryšio sutrikimas | 2.1. Ryšio sutrikimo priežasties nustatymas | 2.1.1. aiškinamasi ryšio sutrikimo priežastis. Jeigu nustatoma, kad ryšys sutriko ne dėl įstaigos įrangos gedimo, kreipiamasi į ryšio paslaugų teikėją dėl ryšio sutrikimo pašalinimo. | Veiklos atkūrimo grupės vadovas |
| | 2.2. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo | 2.2.1. priemonių sutrikimams pašalinti nustatymas. | Veiklos atkūrimo grupės vadovas |

| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
|---|---|---|---|
| | prognozės | | |
| | 2.3. Ryšio sutrikimo pašalinimas | 2.3.1. priemonių sutrikimams pašalinti įgyvendinimas. | Veiklos atkūrimo grupės vadovas |
| 3. Kritinės techninės įrangos gedimas, praradimas (pvz., techninis serverio, duomenų saugyklos, tinklo paskirstymo komponento, tinklo sietuvo, tinklo sąsajos, oro kondicionavi-mo įrangos gedimas, šios įrangos vagystė arba sugadinimas) | 3.1. Situacijos analizė | 3.1.1. identifikuojamas techninės įrangos gedimas, sugadinta ar prarasta techninė įranga; | Veiklos atkūrimo grupės vadovas |
| | | 3.1.2. nustatomi ir įvertinami įvykio padariniai, žala. | Veiklos tęstinumo valdymo grupės vadovas |
| | 3.2. Veiksmų plano sudarymas | 3.2.1. sudaromas veiksmų planas ir, atsižvelgiant į techninės įrangos gedimo, sugadinimo ar praradimo mastą, pasirenkamas optimalus veiklos atkūrimo scenarijus. Galimi veiklos atkūrimo scenarijai:<br>3.2.1.1. naudoti kitos turimos techninės įrangos išteklius;<br>3.2.1.2. kreiptis į techninės įrangos garantinių paslaugų teikėją;<br>3.2.1.3. užsakyti reikalingą techninę įrangą pagal įrangos tiekimo sutartis;<br>3.2.1.4. vykdyti viešąjį techninės įrangos pirkimą;<br>3.2.1.5. atkurti veiklą atsarginėse patalpose (naudoti atsarginėse patalpose esančią infrastruktūrą arba šiose patalpose įrengti reikiamą įrangą);<br>3.2.2. prireikus numatomas finansinių ir kitokių išteklių poreikis informacinės sistemos veiklai atkurti. | Veiklos tęstinumo valdymo grupės vadovas |

| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
|---|---|---|---|
| | 3.3. Padarinių likvidavimas ir veiklos atkūrimas | 3.3.1. informacinės sistemos veikla atkuriama pagrindinėse patalpose arba atsarginėse patalpose pagal pasirinktą veiklos atkūrimo scenarijų. | Veiklos atkūrimo grupės vadovas |
| 4. Stichinė nelaimė, avarija, patalpų praradimas, pažeidimas (pvz., žemės drebėjimas, potvynis, gaisras, | 4.1. Standartinių veiksmų vykdymas | 4.1.1. veiksmų, nustatytų darbuotojų saugos ir sveikatos įvadinėse instrukcijose, vykdymas. | Informacinės sistemos valdytojo, informacinės sistemos tvarkytojo darbuotojai, kiti asmenys |
| sprogimas, teroristinis išpuolis, didelio pavojingų medžiagų kiekio išsiveržimas į aplinką) | | | |
| 5. Patalpų užgrobimas | 5.1. Teisėsaugos institucijų informavimas | 5.1.1. apie neteisėtą įsibrovimą į patalpas informuojamos teisėsaugos institucijos;<br>5.1.2. galimybių evakuoti darbuotojus nagrinėjimas, jei yra teisėsaugos institucijos nurodymas. | Veiklos tęstinumo valdymo grupės vadovas |
| | 5.2. Darbuotojų evakavimas, jei yra teisėsaugos institucijų rekomendacija | 5.2.1. draudimas įeiti į patalpas bet kuriems asmenims, jei yra teisėsaugos institucijos nurodymai;<br>5.2.2. darbuotojų informavimas apie evakavimą. | Veiklos tęstinumo valdymo grupės vadovas |
| | 5.3. Patalpų užrakinimas, jei yra galimybė | 5.3.1. teisėsaugos institucijų nurodymų vykdymas. | Veiklos tęstinumo valdymo grupės vadovas |
| | 5.4. Teisėsaugos institucijų kitų | 5.4.1. darbuotojų informavimas apie nurodymų vykdymą. | Veiklos atkūrimo grupės |

| Situacija | Pirminiai veiksmai | Veiklos atkūrimo veiksmai | Atsakingi vykdytojai |
|---|---|---|---|
| | nurodymų vykdymas, jei yra rekomendacija | | vadovas |
| | 5.5. Veiksmai, atlaisvinus užgrobtas patalpas | 5.5.1. padarytos žalos įvertinimas;<br>5.5.2. padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, darbuotojų instruktavimas ir plano vykdymas. | Veiklos tęstinumo valdymo grupės vadovas, veiklos atkūrimo grupės vadovas |
| 6. Komunalinių paslaugų teikimo sutrikimai (nutrūksta elektros energijos, šildymo, vandens tiekimas) | 6.1. Situacijos analizė | 6.1.1. pagal kompetenciją nustatomos galimos komunalinių paslaugų teikimo sutrikimo priežastys;<br>6.1.2. informuojami komunalinių paslaugų teikėjai. | Veiklos atkūrimo grupės vadovas |
| | 6.2. Veiksmų plano sudarymas | 6.2.1. sudaromas veiksmų planas paslaugų teikimo sutrikimams pašalinti. | Veiklos tęstinumo valdymo grupės vadovas |
| | 6.3. Padarinių likvidavimas ir veiklos atkūrimas | 6.3.1. organizuojamas komunalinių paslaugų teikimo sutrikimų pagal veiksmų planą šalinimas. | Veiklos atkūrimo grupės vadovas |
| 7. Darbuotojų praradimas (pvz., nėra darbuotojų, galinčių vykdyti svarbius įstaigos veiklos procesus) | 7.1. Situacijos analizė | 7.1.1. nustatoma, kokie žmogiškieji ištekliai, būtini svarbiems procesams vykdyti, yra prarasti;<br>7.1.2. nustatoma, kokia darbuotojų kompetencija reikalinga svarbiems procesams vykdyti. | Veiklos atkūrimo grupės vadovas |
| | 7.2. Veiklos atkūrimas | 7.2.1. trūkstamas personalas pakeičiamas pakaitiniais darbuotojais. Prireikus apmokomi esami darbuotojai;<br>7.2.2. vykdomos naujų darbuotojų paieškos ir įdarbinimo procedūros. | Veiklos atkūrimo grupės vadovas |

_____