PATVIRTINTA
Nacionalinio maisto ir veterinarijos
rizikos vertinimo instituto direktoriaus
2022 m. vasario 3 d. įsakymu Nr. 1A-21

NACIONALINIO MAISTO IR VETERINARIJOS RIZIKOS VERTINIMO INSTITUTO TVARKOMŲ REGISTRŲ IR INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinio maisto ir veterinarijos rizikos vertinimo instituto (toliau - NMVRVI) tvarkomų registrų ir informacinių sistemų veiklos tęstinumo valdymo planas (toliau — planas) reglamentuoja Laboratorijos informacijos valdymo sistemos, Kokybės dokumentų informacinės valdymo sistemos, Norminių dokumentų valdymo informacinės sistemos (toliau — IS), elektroninės informacijos tvarkymo veiklos tęstinumo užtikrinimą ir vykdomas įvykus elektroninės informacijos saugos incidentui, kuris gali sudaryti neteisėto prisijungimo prie IS galimybę, sutrikdyti ar pakeisti IS veiklą, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

2. Plane vartojamos sąvokos atitinka sąvokas, apibrėžtas 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 dokumentą turinio gairių apraše, Elektroninės informacijos, sudarančios valstybes informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kiti 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 va1stybės 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 reikalavimų apraše, patvirtintuose Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ ir kituose teisės aktuose.

3. Plano nuostatos taip pat taikomos po stichinės nelaimės, avarijos ar kiti ekstremalių situacijų, kai būtina atkurti įprastą informacinių sistemų veiklą.

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

4.1. informacinių sistemų saugos įgaliotinis (toliau — saugos įgaliotinis), turi teisę pagal savo įgaliojimus:

4.1.1. bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklą, 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 (kibernetinio saugumo) darbo grupės;

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

4.1.3. koordinuoti kibernetinio ir informacinių sistemų elektroninės informacijos saugos incidentų tyrimą.

4.2. informacinių sistemų administratorius (toliau — administratorius):

4.2.1. dalyvauja atliekant plano 15 punkte nurodytas funkcijas;

4.2.2. vykdo kitus plane ir jo priede nurodytus veiksmus ir informacinių sistemų veiklos tęstinumo valdymo grupės ar informacinių sistemų veiklos atkūrimo grupės pavestas užduotis;

4.3. informacinių sistemų tvarkytojas (toliau — tvarkytojas):

4.3.1. įgyvendina IS veiklos atkūrimą;

4.3.2. analizuoja incidento priežastis ir aplinkybes;

4.3.3. įgyvendina elektroninės informacijos fizinės saugos priemones;

4.3.4. skiria finansinius ir fizinius resursus, reikalingus IS veiklai atkurti.

4.4. informacinių sistemų naudotojai vykdo veiklos tęstinumo valdymo grupės nurodymus.

5. Planas privalomas informacinių sistemų valdytojui, tvarkytojui, saugos įgaliotiniui, asmens duomenų saugos pareigūnams, kibernetinio saugumo vadovui, duomenų valdymo įgaliotiniui, administratoriams, informacinių sistemų naudotojams, informacinių sistemų techninės ir programinės įrangos priežiūros funkcijas teikiantiems paslaugų teikėjams, jei tokios funkcijos paslaugų teikėjams perduotos Valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka.

6. Elektroninės informacijos saugos incidento metu patirti nuostoliai IS veiklai atkurti finansuojami valstybės biudžeto, kitomis finansavimu lėšomis.

7. Veiksmų, kurie būtų atliekami įvykus elektroninės informacijos saugos incidentui, vykdymo eiliškumas ir atsakingi vykdytojai nurodyti IS veiklos atkūrimo detaliajame plane (1 priedas).

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

8. Informacinių sistemų veiklos tęstinumui užtikrinti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui sudaromos informacinių sistemų veiklos tęstinumo valdymo grupė (toliau — veiklos tęstinumo valdymo grupė) ir informacinių sistemų veiklos atkūrimo grupė (toliau — veiklos atkūrimo grupė).

9. Veiklos tęstinumo valdymo grupės sudėtis:

9.1. veiklos tęstinumo valdymo grupės vadovas;

9.2. veiklos tęstinumo valdymo grupės vadovo pavaduotojas ir saugos įgaliotinis;

9.3. veiklos tęstinumo valdymo grupės nariai.

10. Veiklos tęstinumo valdymo grupės funkcijos:

10.1. situacijos analizė ir sprendimų informacinių sistemų veiklos tęstinumo valdymo klausimais priėmimas;

10.2. finansinių ir kitų išteklių, reikalingų informacinių sistemų veiklai atkurti įvykus

kibernetiniam ar elektroninės informacijos saugos incidentui, naudojimo kontrolė;

10.3. saugos užtikrinimo atstatymo organizavimas, įvykus elektroninės informacijos saugos ar kibernetinio saugumo incidentui;

10.4. logistikos (asmens, daiktų, įrangos gabenimo) organizavimas ir koordinavimas;

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

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

10.7. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

10.8. informacinių sistemų veiklos atkūrimo priežiūra ir koordinavimas;

10.9. naudotojų, trečiųjų šalių informavimo inicijavimas ir/arba organizavimas.

10.10. kitos veiklos tęstinumo valdymo grupei pavestos funkcijos.

11. Veiklos atkūrimo grupės sudėtis:

11.1. veiklos atkūrimo grupės vadovas;

11.2. veiklos atkūrimo grupės vadovo pavaduotojai;

11.3. veiklos atkūrimo grupės nariai:

11.3.1 NMVRVI administratorius;

11.3.2 NMVRVI saugos įgaliotinis;

11.3.3 NMVRVI atsakingas asmuo.

12. Veiklos atkūrimo grupės funkcijos:

12.1. tarnybinių stočių veikimo atkūrimo organizavimas;

12.2. kompiuterio tinklo veikimo atkūrimo organizavimas;

12.3. informacinių sistemų ir registrų elektroninės informacijos atkūrimo organizavimas;

12.4. taikomųjų programų ir duomenų bazių tinkamo veikimo atkūrimo organizavimas;

12.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterinio tinklo organizavimas;

12.6. naudotojų ir trečiųjų šalių informavimas;

12.7. kitos veiklos atkūrimo valdymo grupei pavestos funkcijos.

13. Personalinę veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės sudėtį tvirtina NMVRVI direktorius.

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

15. Veiklos tęstinumo valdymo ir atkūrimo grupių nariai turi reaguoti ir valdyti incidentus vadovaudamiesi 1 priede pateiktu veiksmų aprašymu;

16. Informacinių sistemų veiklos atkūrimo detalusis planas pateikiamas šio plano 1 priede.

17. Atsarginėms patalpoms, naudojamoms informacinių sistemų veiklai atkurti, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, keliami šie reikalavimai:

17.1. patalpos turi atitikti priešgaisrinės saugos reikalavimus;

17.2. patalpos turi atitikti informacinių sistemų techninės įrangos gamintojo nustatytus reikalavimus įrangos darbo aplinkai (pvz., tinkama oro temperatūra, oro drėgmė ir kt.);

17.3. patalpose turi būti įrengtos langų, durų, informacinių sistemų techninės įrangos, kabelių fizinės apsaugos priemonės;

17.4. patalpose turi būti įrengta patalpų apsaugos signalizacija, prijungta prie apsaugos tarnybų stebėjimo sistemų;

17.5. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

17.6. patalpose turi būti interneto ryšio prieiga;

17.7. patalpose turi būti įrengti nenutrūkstamą elektros tiekimą užtikrinantys maitinimo šaltiniai;

17.8. turi būti įdiegtos kitos reikalingos priemonės, atitinkančios atitinkamų kategorijų informacinių sistemų veiklai ir jų saugumui užtikrinti keliamus reikalavimus.

18. Veiklos tęstinumo valdymo grupė, atlikusi situacijos analizę, nedelsiant informuoja veiklos atkūrimo grupę apie priimtus sprendimus informacinių sistemų veiklos tęstinumo valdymo klausimais. Veiklos atkūrimo grupė, atsižvelgdama į priimtus sprendimus, organizuoja informacinių sistemų veiklos atkūrimą.

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

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

25. Informacinių sistemų veiklos tęstinumui užtikrinti NMVRVI turi būti parengti ir saugomi šie dokumentai:

25.1. kiekvieno pastato, kuriame yra informacinių sistemų įranga, aukštų patalpų brėžiniai ir juose pažymėta:

25.1.1. tarnybinės stotys;

25.1.2. kompiuterizuotos darbo vietos;

25.1.3. kompiuterių tinklo ir telefonų tinklo mazgai;

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

25.1.5. elektros įvedimo pastate vietos;

25.1.6. informacinių sistemų kompiuterių tinklo fizinio ir loginio sujungimo schemos.

25.2. kompiuterinės, techninės ir programinės įrangos sutarčių sąrašas;

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

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

25.5. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos informacinių sistemų valdytojo ir tvarkytojo poreikius atitinkančiai informacinių sistemų 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 informacinių sistemų veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą;

25.6. elektroninės informacijos teikimo sutarčių sąrašas ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigas;

26. Už plano 25.1-25.6 papunkčiuose nurodytų dokumentų parengimą, saugojimą, nuolatinį atnaujinimą ir kompiuterinės, techninės ir programinės įrangos sutarčių vykdymo priežiūrą atsakingi informacinių sistemų administratoriai.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

27. Reguliarius plano veiksmingumo išbandymus organizuoja informacijos saugos įgaliotinis.

28. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus kibernetinio ar elektroninės informacijos saugos incidento ar nenumatytos situacijos simuliacijos metu.

29. Kibernetinio ar elektroninės informacijos saugos incidento metu gauti rezultatai turi būti naudojami planui atnaujinti. Nustačius plano veiksmingumo trūkumą, rengiama pastebėtų trūkumų šalinimo ataskaita. Už plano veiksmingumo išbandymo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą informacinių sistemų valdytojui atsakingas informacijos saugos įgaliotinis. Plano veiksmingumo išbandymo ataskaitos šablonas yra pateiktas šio plano 2 priede.

30. Plano veiksmingumo išbandyme turi dalyvauti visi veiklos tęstinumo valdymo grupės nariai.

31. Atsižvelgdamas į plano veiksmingumo išbandymo metu pastebėtus trūkumus, saugos įgaliotinis veiklos tęstinumo valdymo grupei turi pateikti siūlymus dėl plano pakeitimų arba papildymų.

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

33. Remiantis Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.2 papunktyje nurodytu reikalavimu, Veiklos tęstinumo valdymo plano išbandymo ataskaitų kopijos ne vėliau kaip per penkias darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

_____

Nacionalinio maisto ir veterinarijos rizikos vertinimo instituto tvarkomų informacinių sistemų veiklos tęstinumo valdymo plano

1 priedas

NACIONALINIO MAISTO IR VETERINARIJOS RIZIKOS VERTINIMO INSTITUTO TVARKOMŲ REGISTRŲ IR INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

1. NMVRVI tvarkomų registrų ir informacinių sistemų veiklos atkūrimo detaliajame plane (toliau — atkūrimo planas) reglamentuojamas registrų ir informacinių sistemų atkūrimo veiksmų vykdymo eiliškumas, nurodomi atsakingi vykdytojai.

2. Įsigaliojus NMVRVI tvarkomų registrų ir informacinių sistemų veiklos tęstinumo valdymo planui veiklos tęstinumo valdymo grupės įgalioti asmenys informuoja informacinių sistemų naudotojus, susijusių registrų ir kitų informacinių sistemų tvarkytojus, kitus suinteresuotus asmenis apie informacinių sistemų veikimo sutrikimus. Informuojama gali būti pranešimu NMVRVI interneto svetainėje, informacinių sistemų taikomosiose programose, kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir pan.).

3. Veiklos atkūrimo grupė informacinių sistemų veiklą atkuria pagal šiuos informacinių sistemų funkcijų prioritetus ir kategorijas (pirmiausia atkuriama aukštesnės kategorijos informacinės sistemos veikla):

3.1. interneto ryšio atkūrimas; tarnybinių stočių veikimo atkūrimas;

3.2. kompiuterio tinklo veikimo atkūrimas;

3.3. duomenų bazių veikimo atkūrimas; taikomųjų programų veikimo atkūrimas;

3.4. elektroninės informacijos atkūrimas;

3.5. kompiuterinių darbo vietų veikimo atkūrimas.

4. Informacinių sistemų veiklos atkūrimo veiksmai, atsižvelgiant į kibernetinio ar elektroninės informacijos saugos incidento tipą ir mastą, veiklos atkūrimo veiksmą pobūdį turi būti atlikti per kuo trumpesnį terminą. Informacinių sistemų veiklos atkūrimo veiksmai nurodyti lentelėje.

Lentelė

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
1. Kibernetinė ataka, įskaitant manipuliaciją elektronine informacija (pvz., elektroninės informacijos, įskaitant informacinių sistemų programinę įrangą, pakeitimas kita elektronine informacija, elektroninės informacijos iškraipymas, ištrynimas ar kitoks neteisėtas jos naudojimas).	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. 1.1.2 Stabdomas pažeistos elektroninės informacijos teikimas. 1.1.3.Nustatomos elektroninės informacijos vientisumo pažeidimo, neteisėto tvarkymo priežastys. 1.1.4. Nustatoma poveikio reikšmė bei nustatoma incidento kategorija. 1.1.5. Informuojamos kompetentingos institucijos, kitos suinteresuotos šalys. 1.1.6. Įvertinus poveikio reikšmę, nustatomas NKSC informavimo modelis: **didelio poveikio kibernetinis incidentas** – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo; **vidutinio poveikio kibernetinis incidentas** – ne vėliau kaip per keturias valandas nuo jų nustatymo; **nereikšmingo poveikio kibernetinis incidentas** – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.	Veiklos atkūrimo grupė
	1.2. Veiksmų plano sudarymas.	1.2.1. Sudaromas veiksmų planas kibernetinės atakos padariniams likviduoti, informacinių sistemų veiklai atkurti ir informacinėms sistemoms 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. 1.3.2 Likviduojami kibernetinio ar elektroninės informacijos saugos incidento padariniai, atkuriamas informacinių sistemų veikimas, diegiamos informacinių sistemų apsaugos priemonės. 1.3.3 Jeigu informacinių sistemų veiklos atkūrimo metu elektroninė informacija atkuriama iš atsarginių kopiją, tikrinama, ar atkurta elektroninė informacija yra teisinga. 1.3.4. Jeigu nėra galimybės elektroninės informacijos tinkamai atkurti iš atsarginių kopijų, duomenų teikėjų prašoma pateikti elektroninę informaciją iš naujo. 1.3.5. Atkuriamas elektroninės informacijos paslaugų teikimas. 1.3.6. Prireikus veikla atkuriama atsarginėse patalpose.	Veiklos atkūrimo grupė
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 prognozės.	2.2.1. Priemonių nustatymas sutrikimams pašalinti.	Veiklos atkūrimo grupės vadovas
	2.3. Ryšio sutrikimo pašalinimas.	2.3.1. Priemonių įgyvendinimas.	Veiklos atkūrimo grupės vadovas
3. Kritinės techninės įrangos gedimas, praradimas (pvz., techninis serverio, duomenų, saugyklos, tinklo paskirstymo komponento, tinklo sietuvo, tinklo sąsajos, oro kondicionavimo įrangos gedimas, šios įrangos vagystė arba	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

sugadinimas).			
	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: 3.2.1.1 naudoti kitos turimos techninės įrangos išteklius; 3.2.1.2. kreiptis į techninės įrangos garantinių paslaugų teikėją; 3.2.1.3. užsakyti reikalingą techninę įrangą pagal įrangos tiekimo sutartis; 3.2.1.4. vykdyti viešąjį techninės įrangos pirkimą; 3.2.1.5. atkurti veiklą atsarginėse patalpose (naudoti atsarginėse patalpose esančią infrastruktūrą arba šiose patalpose įrengti reikiamą įrangą). 3.2.2. Prireikus numatomas finansinių ir kitokių išteklių poreikis informacinių sistemų veiklai atkurti.	Veiklos tęstinumo valdymo grupės vadovas
	3.3. Padarinių likvidavimas ir veiklos atkūrimas.	3.3.1. Informacinių sistemų veikla atkuriama pagrindinėse patalpose arba atsarginėse patalpose pagal pasirinktą veiklos atkūrimo scenarijų.	Veiklos atkūrimo grupės vadovas
4. Pagrindinių duomenų praradimas pažeidus ar kitaip sugadinus centrinę duomenų saugyklą	4.1. Paslaugų teikimo naudotojams nutraukimas, jeigu tai kelia pavojų prarasti duomenis ir kitaip pažeisti programinės įrangos funkcionalumą;	4.1.1. Informuoti naudotojus apie paslaugų teikimo nutraukimą; 4.1.2. Nutraukti paslaugas; 4.1.3. Jeigu duomenys prarasti arba tapo prieinami leidimo/įgaliojimų neturintiems asmenims, pranešti saugos įgaliotiniui, taip pat teisėsaugos organams; 4.1.4. Teikti informaciją apie įvykį teisėsaugos organams, vykdyti teisėsaugos organų nurodymus;	Veiklos tęstinumo valdymo grupė
	4.2. Atkurti informacinės sistemos ir/arba registro darbingumą;	4.2.1 Atkurti informacinės sistemos ir/arba registro darbingumą; 4.2.2. Nustatyti, ar atkurti duomenys yra patikimi.	Veiklos atkūrimo grupė
5. Stichinė nelaimė, avarija, patalpą praradimas, pažeidimas	5.1. Standartinių veiksmų vykdymas.	5.1.1. Veiksmų, nustatytų darbuotojų saugos ir sveikatos įvadinėse instrukcijose, vykdymas.	Informacinių sistemų valdytojo, informacinių sistemų

(pvz., žemės drebėjimas, potvynis, gaisras, sprogimas, teroristinis išpuolis, didelio kiekio pavojingą medžiagų išsiveržimas į aplinką).			tvarkytojo darbuotojai, kiti asmenys
6. Patalpų užgrobimas.	6.1. Teisėsaugos institucijų informavimas.	6.1.1. Apie neteisėtą įsibrovimą į patalpas informuojamos teisėsaugos institucijos. 6.1.2. Galimybių evakuoti darbuotojus analizė, jei yra teisėsaugos institucijos nurodymas.	Veiklos tęstinumo valdymo grupės vadovas
	6.2. Darbuotojų evakavimas, jei yra teisėsaugos institucijų rekomendacija.	6.2.1. Draudimas įeiti į patalpas bet kuriems asmenims, jei yra teisėsaugos institucijos nurodymai. 6.2.2. Darbuotojų informavimas apie evakavimą.	Veiklos tęstinumo valdymo grupės vadovas
	6.3. Patalpų užrakinimas, jei yra galimybė.	6.3.1. Teisėsaugos institucijų nurodymų vykdymas.	Veiklos tęstinumo valdymo grupės vadovas
	6.4. Teisėsaugos institucijų kitų nurodymų vykdymas, jei yra rekomendacija.	6.4.1. Darbuotojų informavimas apie nurodymų vykdymą.	Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovas
	6.5 Veiksmai atlaisvinus užgrobtas patalpas.	6.5.1. Padarytos žalos įvertinimas. 6.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, darbuotojų instruktavimas ir plano vykdymas.	
7. Komunalinių paslaugų teikimo sutrikimai (nutrūksta elektros energijos, šildymo, vandens tiekimas).	7. 1. Situacijos analizė.	7.1.1. Pagal kompetenciją nustatomos galimos komunalinių paslaugų tiekimo sutrikimo priežastys. 7.1.2. Informuojami komunalinių paslaugų teikėjai.	Veiklos atkūrimo grupės vadovas
	7.2. Veiksmo plano sudarymas.	7.2.1. Sudaromas veiksmų planas paslaugų teikimo sutrikimams pašalinti.	Veiklos tęstinumo valdymo grupės vadovas
	7.3. Padarinių likvidavimas ir veiklos atkūrimas.	7.3.1. Organizuojamas komunalinių paslaugų teikimo sutrikimo pagal veiksmų planą šalinimas.	Veiklos atkūrimo grupės vadovas

8. Darbuotojų praradimas (pvz., nėra darbuotojų, galinčių vykdyti svarbius įstaigos veiklos procesus).	8.1. Situacijos analizė.	8.1.1. Nustatoma, kokie žmogiškieji ištekliai, būtini svarbiems procesams vykdyti, yra prarasti. 8.1.2. Nustatoma, kokia darbuotojų kompetencija reikalinga svarbiems procesas vykdyti.	Veiklos atkūrimo grupės vadovas
	8.2. Veiklos atkūrimas.	8.2.1.Trūkstamas personalas pakeičiamas pakaitiniais darbuotojais. Prireikus apmokomi esami darbuotojai. 8.2.2.Vykdomos naujų darbuotojų paieškos ir atliekamos įdarbinimo procedūros.	Veiklos atkūrimo grupės vadovas

Nacionalinio maisto ir veterinarijos
rizikos vertinimo instituto tvarkomų
informacinių sistemų veiklos
tęstinumo valdymo plano
2 priedas

VEIKLOS TĘSTINUMO VALDYMO PLANO
VEIKSMINGUMO IŠBANDYMO ATASKAITA
(Veiklos tęstinumo valdymo grupės susitikimo data ir dokumento numeris)

Veiklos tęstinumo valdymo plano veiksmingumo išbandyme dalyvavo:
1. _____
2. _____
3. _____
...

Elektroninės informacijos saugos incidento scenarijaus apibūdinimas:
_____

Elektroninės informacijos saugos incidento paveiktos funkcijos ir posistemiai:
_____

Elektroninės informacijos saugos incidento šalinimo eiga:
_____

Pastebėti veiklos tęstinumo valdymo plano trūkumai:
_____

Siūlomi prevenciniai veiksmai pastebėtiems trūkumams šalinti:
_____

Siūlymai dėl veiklos tęstinumo valdymo plano keitimo:
_____

(vardas, pavardė) (parašas)

(vardas, pavardė) (parašas)

(vardas, pavardė) (parašas)

_____