

PATVIRTINTA
Lietuvos Respublikos aplinkos ministro
2012 m. liepos 25 d. įsakymu Nr.D1-637
(Lietuvos Respublikos aplinkos ministro
2016 m. vasario 19 d. įsakymo Nr. D1-
123 redakcija)

LIETUVOS RESPUBLIKOS APLINKOS MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos aplinkos ministerijos (toliau – Ministerija) informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Planas) nustato Ministerijos informacinių sistemų (toliau – Informacinės sistemos), nurodytų Informacinių sistemų duomenų saugos nuostatuose (toliau – Saugos nuostatai), veiklos tęstinumo organizacines, aprašomasias ir Plano veiksmingumo išbandymo nuostatas. Plano reikalavimai yra privalomi Informacinių sistemų tvarkytojams, valdytojui, Saugos įgaliotiniams, Administratoriams ir Naudotojams. Planas įsigalioja įvykus elektroninės informacijos saugos incidentui.

2. Plane vartojamos sąvokos atitinka teisės aktuose, kuriais vadovaujantis Planas yra parengtas, ir kituose saugų elektroninės informacijos tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

3. Planui įgyvendinti nustatomos funkcijos ir įgaliojimai:

3.1. Informacinės sistemos saugos įgaliotinis dalyvauja Veiklos tęstinumo valdymo grupėje ir teikia jai informaciją apie elektroninės informacijos saugos incidentus;

3.2. Administratoriai užtikrina informacinių sistemų atkūrimą ir dalyvauja Veiklos atkūrimo grupės veikloje;

3.3. Informacinių sistemų Naudotojai privalo vykdyti Plano ir Veiklos tęstinumo valdymo grupės reikalavimus.

4. Informacinių sistemų veikla, įvykus elektroninės informacijos saugos incidentui, atkuriamą valstybės biudžeto ir kitomis lėšomis.

5. Informacinių sistemų veikla laikoma atkurta, jeigu yra atkurtas elektroninės informacijos saugos incidento metu sutrikęs Informacinių sistemų prieinamumas, užtikrintas duomenų konfidencialumas ir vientisumas.

6. Informacinių sistemų neveikimo laikotarpis negali būti ilgesnis nei 16 val.

7. Per metus turi būti užtikrintas Informacinių sistemų prieinamumas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis.

II. ORGANIZACINĖS NUOSTATOS

8. Veiklos tęstinumo valdymo grupę sudaro:

8.1. Ministerijos kancleris (Veiklos tęstinumo valdymo grupės vadovas);

8.2. Ministerijos Informacinių technologijų skyriaus vedėjas (Veiklos tęstinumo valdymo grupės vadovo pavaduotojas);

8.3. Informacinės sistemos tvarkytojo įgaliotas asmuo;

8.4. Ministerijos Bendrųjų reikalų skyriaus vedėjas;

8.5. Ministerijos saugos įgaliotinis;

8.6. Informacinės sistemos saugos įgaliotinis (jeigu Informacinė sistema priskirta ne Ministerijos saugos įgaliotiniui);

8.7. kiti asmenys gali būti pasitelkiami pagal poreikį.

9. Veiklos tęstinumo valdymo grupės funkcijos:

9.1. susitikimo metu vertina elektroninės informacijos saugos incidentą ir, jei reikia, skelbia (grupės vadovas) ekstremaliąją situaciją;

9.2. vykdo situacijos analizę ir priima sprendimus, susijusius su Informacinių sistemų veiklos tęstinumo valdymo užtikrinimu;

9.3. skiria ir kontroliuoja, kaip naudojami finansiniai ištekliai, reikalingi veiklos tęstinumui atkurti;

9.4. pagal elektroninės informacijos saugos incidento pobūdį sudaro Ministerijos Veiklos atkūrimo grupę;

9.5. bendrauja su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

9.6. bendrauja su kitomis valstybės institucijomis ir įstaigomis, kitomis interesų grupėmis;

9.7. bendrauja su teisėsaugos institucijomis;

9.8. organizuoja ir užtikrina fizinę saugą;

9.9. organizuoja žmonių, daiktų, įrangos gabenimą į saugią vietą.

10. Veiklos atkūrimo grupę sudaro:

10.1. Ministerijos Informacinių technologijų skyriaus vyriausiasis specialistas (Atkūrimo grupės vadovas);

10.2. Informacinės sistemos saugos įgaliotinis (Atkūrimo grupės vadovo pavaduotojas);

10.3. Informacinės sistemos administratorius;

10.4. kiti darbuotojai ar išoriniai ekspertai pasitelkiami pagal poreikį.

11. Veiklos atkūrimo grupės funkcijos:

11.1. Informacinių sistemų veiklos atkūrimo priežiūra ir koordinavimas (Atkūrimo grupės vadovas; Informacinės sistemos saugos įgaliotinis);

11.2. tarnybinių stočių veiklos atkūrimas ir jų priežiūra (Informacinės sistemos saugos įgaliotinis; Informacinės sistemos administratorius);

11.3. vidaus duomenų perdavimo tinklo veiklos atkūrimas ir jo priežiūra (Informacinės sistemos saugos įgaliotinis; Informacinės sistemos administratorius);

11.4. taikomųjų programų veiklos atkūrimas ir jų priežiūra (Informacinės sistemos saugos įgaliotinis; Informacinės sistemos administratorius);

11.5. kitos Veiklos tęstinumo valdymo grupės pavestos funkcijos.

12. Esant paskelbtai ekstremaliajai situacijai, Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė organizuoja pasitarimus, atsižvelgdamos į Veiklos tęstinumo valdymo grupės susitikimų metu nustatytą dažnumą, palaiko ryšius visomis tuo metu prieinamomis priemonėmis (el. paštu, mobiliuoju ryšiu ir kt.).

13. Reaguojant į elektroninės informacijos saugos incidentus ir juos valdant, turi būti vadovaujamosi veiksmais, išdėstytais Detaliajame ekstremaliosios situacijos valdymo ir veiklos atkūrimo plane (1 priedas), ir šiais principais:

13.1. Naudotojų gyvybės ir sveikatos apsauga. Būtina užtikrinti visų darbuotojų gyvybės ir sveikatos apsaugą, kol trunka ekstremali situacija ir likviduojami elektroninės informacijos saugos incidento padariniai;

13.2. Informacinių sistemų veiklos atkūrimas. Paskelbus ekstremaliąją situaciją, jei būtina, organizuojama fizinė sauga ir veiklos atkūrimas. Pirmiausia atkuriamos kritiškiausios Informacinės sistemos ir užtikrinamas jų prieinamumas;

13.3. Plano arba jo dalių veiksmingumas. Plano arba jo dalių veiksmingumas turi būti reguliariai išbandomas Veiklos tęstinumo valdymo grupės iniciatyva ir, jei būtina, tikslinamas, atsižvelgiant į nustatytus trūkumus.

14. Per ekstremalią situaciją sunaikinta techninė, sisteminė ir taikomoji programinė įranga keičiama turima rezervine arba testine Informacinių sistemų aplinkos įranga, vėliau įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo ištekliai padengiami iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių.

15. Atsarginių patalpų, naudojamų veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, reikalavimai:

- 15.1. patekimas į patalpas turi būti registruojamas žurnale;
- 15.2. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;
- 15.3. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės;
- 15.4. patalpose turi būti įrengtas rezervinis elektros energijos šaltinis informacinių sistemų techninei įrangai ir duomenų perdavimo tinklo mazgams, užtikrinantis įrangos veikimą ne trumpiau kaip 10 minučių;
- 15.5. ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo;
- 15.6. patalpoje turi nuolat veikti oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema);
- 15.7. Atsarginių patalpų, naudojamų Informacinių sistemų veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, adresas, ir, kaip jas rasti, nurodytas 3 priede.

III. APRAŠOMOSIOS NUOSTATOS

16. Veiklos tęstinumo vykdymui užtikrinti turi būti surinkta ir naudojama detali bei aktuali informacija, būtina informacinių sistemų veiklai atkurti.

17. Detalios informacijos, būtinos veiklos tęstinumui, aprašo rengimą ir atnaujinimą organizuoja informacinių sistemų administratoriai. Detalią informaciją sudaro:

17.1. Techninės ir programinės įrangos dokumentacija (product manual), kurioje nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas (-i) administratorius (administratoriai), minimalus informacinės sistemos veiklai atkurti, kai nėra administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis;

17.2. kompiuterinės įrangos instrukcija, kurioje nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui, specifikacija;

17.3. pastatų planai, kuriuose nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti:

17.3.1. tarnybinės stotys;

17.3.2. kompiuterių tinklo ir telefonų tinklo mazgai;

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

17.3.4. elektros įvedimo pastate vietos;

17.4. tinklo planas, kuriame nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemas;

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

17.6. programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

17.7. dokumentas, kuriame nurodytas veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis.

IV. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

18. Už Plano veiksmingumo išbandymą ir jo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą Veiklos tęstinumo valdymo grupės vadovui atsakingas informacinių sistemų administratorius.

19. Planas turi būti išbandomas esant esminiams Informacinių sistemų pokyčiams, bet ne rečiau kaip kartą per dvejus metus. Plano bandymo metu Veiklos tęstinumo valdymo grupė išanalizuoja galimą (sumodeliuotą) elektroninės informacijos saugos incidentą, numato galimus jos valdymo būdus, galimus sprendimus ir parengia Plano bandymo ataskaitą pagal Ministerijos informacinių sistemų veiklos tęstinumo valdymo eigos (plano bandymo) ataskaitos formą (2 priedas).

20. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

21. Po Plano išbandymo ir (ar) rizikos veiksnių įvertinimo prireikus planas atnaujinamas.

DETALUSIS EKSTREMALIOSIOS SITUACIJOS VALDYMO IR INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO PLANAS

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
1. Gamtos stichijos	1.1. galimos žalos Informacinei sistemai įvertinimas, priemonių plano užkirsti kelią elektroninės informacijos saugos incidentui (toliau – saugos incidentas) sudarymas ir įgyvendinimas;	1.1.1. žalos įvertinimas, priemonių plano saugos incidento pasekmėms likviduoti sudarymas ir įgyvendinimas;	Veiklos tęstinumo valdymo grupės vadovas
	1.2. Informacinės sistemos veiklos atkūrimo veiksmus atliekančių darbuotojų paskyrimas, jų budėjimo grafiko nustatymas ir jų informavimas apie tai;	1.2.1. darbų grafiko saugos incidento pasekmėms likviduoti sudarymas; 1.2.2. saugos incidento pasekmių likvidavimo darbams atlikti darbuotojų sąrašo sudarymas ir jų informavimas apie tai;	Informacinės sistemos administratorius Veiklos atkūrimo grupės vadovas Informacinės sistemos administratorius
	1.3. meteorologinės informacijos sekimas;	1.3.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų informavimas apie esamą situaciją;	Informacinės sistemos saugos įgaliotinis
	1.4. Informacinės sistemos naudotojams rekomenduojamo elgesio saugos incidento metu skelbimas žodžiu arba ryšio priemonėmis;	1.4.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų instruktavimas apie elgseną saugos incidento vietoje;	Informacinės sistemos saugos įgaliotinis

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
	1.5. saugios vietos nustatymas ir nurodymas Informacinės sistemos naudotojams eiti į saugią vietą;	1.5.1. Informacinės sistemos naudotojų informavimas apie būtinumą pereiti į kitas saugias patalpas;	Veiklos tęstinumo valdymo grupės vadovas
	1.6. Informacinės sistemos naudotojų informavimas apie darbo sustabdymą dėl nepalankių sąlygų; <hr/> 1.7. pasiruošimas suteikti nukentėjusiems Informacinės sistemos naudotojams pirmąją pagalbą;	1.6.1. Informacinės sistemos naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas; <hr/> 1.7.1. pirmos pagalbos suteikimas nukentėjusiems Informacinės sistemos naudotojams, nukentėjusių gabenimo į gydymo įstaigą organizavimas;	Informacinės sistemos saugos įgaliotinis <hr/> Informacinės sistemos administratorius
	1.8. pavojingų vietų ženklavimas, informacinių lentelių pakabinimas; <hr/> 1.9. alternatyvių energijos tiekimo šaltinių panaudojimas; <hr/> 1.10. alternatyvaus ryšio organizavimas; <hr/> 1.11. pagrindinės Informacinės sistemos techninės ir programinės įrangos, duomenų galimam pavojui išvengti / likviduoti paruošimas;	1.8.1. Informacinės sistemos naudotojų informavimas, saugos incidento pasekmes likviduojančių darbuotojų instruktavimas; <hr/> 1.9.1. energijos tiekimo tarnybų rekomendacijų vykdymas; <hr/> 1.10.1. kreipimasis į ryšio paslaugos teikėjus; <hr/> 1.11.1. Informacinės sistemos tarnybinių stočių, kitos techninės įrangos išjungimas;	Informacinės sistemos saugos įgaliotinis <hr/> Veiklos atkūrimo grupės vadovas <hr/> Veiklos atkūrimo grupės vadovas <hr/> Informacinės sistemos administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
2. Gaisras	2.1. esant būtinumui, Informacinės sistemos naudotojų evakuacija;	2.2.1. galimybių evakuoti Informacinės sistemos naudotojus nagrinėjimas,	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis
	2.2. priešgaisrinės apsaugos ir gelbėjimo tarnybos informavimas;	2.2.1. priešgaisrinės ir gelbėjimo tarnybos paklausimas dėl leidimo dirbti saugos incidento zonoje, rekomendacijų darbui gavimas, Informacinės sistemos naudotojų informavimas apie rekomenduojamus darbo būdus;	Informacinės sistemos saugos įgaliotinis
	2.3. gaisro gesinimas ankstyvoje stadijoje, nekeliant pavojaus Informacinės sistemos naudotojų gyvybei;	2.3.1. priešgaisrinės ir gelbėjimo tarnybos nurodymų vykdymas;	Informacinės sistemos administratorius
	2.4. komunalinių komunikacijų, galinčių sukelti papildomą nenumatytą situaciją, išjungimas;	2.4.1. priešgaisrinės ir gelbėjimo tarnybos rekomendacijų vykdymas;	Informacinės sistemos administratorius
	2.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 punktuose, atlikimas;	2.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
3. Patalpų, kuriose yra Informacinės sistemos tarnybinės stotys ir svarbiausia komutacinė įranga (toliau – patalpos) užgrobimas	3.1. teisėsaugos tarnybų informavimas;	3.1.1. teisėsaugos tarnybų informavimas apie saugos incidentą;	Veiklos tęstinumo valdymo grupės vadovas
	3.2. esant būtinumui, visų konkrečioje situacijoje nereikalingų Informacinės sistemos naudotojų evakavimas, įspėjant teisėsaugos tarnybas;	3.2.1. Informacinės sistemos naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų rekomendacija;	Informacinės sistemos saugos įgaliotinis
	3.3. esant būtinumui, Informacinės sistemos techninės įrangos išjungimas ir patalpų užrakinimas;	3.3.1. Informacinės sistemos tarnybinių stočių, kitos techninės įrangos išjungimas, patalpų užrakinimas, jei yra galimybė;	Informacinės sistemos administratorius
	3.4. esant būtinumui, likusių Informacinės sistemos naudotojų evakavimas;	3.4.1. Informacinės sistemos naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų rekomendacija;	Informacinės sistemos saugos įgaliotinis
	3.5. teisėsaugos pareigūnų nurodymų vykdymas;	3.5.1. Informacinės sistemos naudotojų informavimas apie teisėsaugos tarnybų nurodymus;	Informacinės sistemos saugos įgaliotinis
	3.6. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 punktuose, atlikimas;	3.6.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
4. Patalpų sugadinimas	4.1. avarinių ar teisėsaugos tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį;	4.1.1. atitinkamos tarnybos paklausimas dėl leidimo dirbti pavojaus zonoje, rekomendacijų darbui gavimas, IS naudotojų informavimas apie rekomenduojamus darbo būdus;	Informacinės sistemos saugos įgaliotinis
	4.2. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 punktuose, atlikimas;	4.2.1. veiksmų, nurodytų šios priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius
	4.3. esant reikalui, atsarginių patalpų IS veiklai užtikrinti ir darbo vietoms išdėstyti suradimas;	4.3.1. darbo organizavimas ir koordinavimas atsarginėse Informacinės sistemos patalpose;	Veiklos atkūrimo grupės vadovas
	4.4. komunalinių komunikacijų, galinčių sukelti papildomą saugos incidentą, išjungimas;	4.4.1. pažeistų patalpų rekonstrukcijos, atstatymo darbų, komunalinių komunikacijų išjungimo organizavimas ir / ar Informacinės sistemos perkėlimas į naujas patalpas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas
5. Elektros energijos tiekimo sutrikimai	5.1. elektros energijos tiekimo sistemos veiklos patikrinimas;	5.1.1. pažeisto vietos elektros tinklo, užtikrinančio Informacinės sistemos veiklą, atkūrimo organizavimas;	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
	5.2. esant būtinumui, tarnybinių stočių ir kitos techninės įrangos, jautrios elektros energijos tiekimo sutrikimams, išjungimas;	5.2.1. elektros energijos tiekimo Informacinės sistemos tarnybinėms stotims ir kitai techninei įrangai išjungimas;	Veiklos atkūrimo grupės vadovas Informacinės sistemos administratorius
	5.3. kreipimasis į savo elektros energijos tiekimo tarnybą dėl sutrikimo pašalinimo trukmės prognozės;	5.3.1. rekomendacijų iš elektros energijos tiekimo tarnybos gavimas;	Veiklos atkūrimo grupės vadovas
	5.4. sutrikimo pašalinimo trukmės prognozės skelbimas Informacinės sistemos naudotojams;	5.4.1. Informacinės sistemos naudotojų informavimas apie esamą situaciją bei numatomas darbo sąlygas;	Informacinės sistemos saugos įgaliotinis
	5.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.10, 6.3 punktuose, atlikimas;	5.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.10.1, 4.3.1 punktuose, vykdymas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius
6. Ryšio sutrikimai	6.1. ryšio sutrikimo priežasčių nustatymas;	6.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Informacinės sistemos administratorius
	6.2. telefono ir / ar interneto ryšio paslaugų teikėjų informavimas, atsižvelgus į sutrikimo pobūdį, paklausimo dėl jo pašalinimo trukmės prognozės pateikimas;	6.2.1. kreipimasis į telefono ir / ar interneto paslaugų teikėjus;	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
	6.3. sutrikimo pašalinimo prognozės skelbimas Informacinės sistemos naudotojams;	6.3.1. Informacinės sistemos naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	Informacinės sistemos saugos įgaliotinis
	6.4. alternatyvaus ryšio organizavimas;	6.4.1. neatkūrus ryšio per prognozuotą laiką, ryšio per kitus ryšio paslaugų teikėjus organizavimas;	Veiklos atkūrimo grupės vadovas Informacinės sistemos administratorius
7. Informacinės sistemos tarnybinių stočių ar komutacinės įrangos sugadinimas (gedimas), sunaikinimas, praradimas	7.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 punktuose, atlikimas;	7.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius
	7.2. rezervinės Informacinės sistemos techninės įrangos naudojimas;	7.2.1. esant būtinumui, teisės aktų nustatyta tvarka informuojamos atsakingos institucijos dėl Informacinės sistemos techninės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas;	Veiklos atkūrimo grupės vadovas
		7.2.2. pranešimas draudimo įstaigai apie įvykį, dėl kurio nukentėjo apdrausti daiktai;	Veiklos tęstinumo grupės vadovas
		7.2.3. esamos techninės įrangos išteklių perskirstymas Informacinės sistemos	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
		veiklai užtikrinti;	
		7.2.4. esant būtinumui, kreipimasis į techninės įrangos tiekėjus dėl sugadintos įrangos remonto ar dėl naujos techninės įrangos įsigijimo;	Veiklos atkūrimo grupės vadovas
8. Informacinės sistemos programinės įrangos sugadinimas, praradimas	8.1. veiksmy, nurodyty šio priedo 1.1, 1.2, 1.4 punktuose, atlikimas;	8.1.1. veiksmy, nurodyty šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius
	8.2. Informacinės sistemos programinės įrangos atkūrimas iš atsarginių kopijų;	8.2.1. esant būtinumui, teisės aktų nustatyta tvarka informuojamos atsakingos institucijos ir vykdomi tolimesni jų nurodymai;	Veiklos tęstinumo valdymo grupės vadovas
		8.2.2. sugadintos ar prarastos programinės įrangos atkūrimas iš programinės įrangos kopijų;	Informacinės sistemos administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinės sistemos veiklos atkūrimo veiksmai	Informacinės sistemos veiklos atkūrimo veiksmų atsakingi vykdytojai
9. Informacinės sistemos duomenų pakeitimas, sunaikinimas, atskleidimas	9.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 punktuose, atlikimas.	9.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 punktuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius
		9.1.2. įvykus neteisėtam Informacinės sistemos duomenų pakeitimui, sunaikinimui ar atskleidimui, teisės aktų nustatyta tvarka informuojamos atsakingos institucijos ir vykdomi tolimesni jų nurodymai;	Veiklos tęstinumo valdymo grupės vadovas
		9.1.3. Informacinei sistemai nustojus funkcionuoti dėl duomenų pakeitimo ar sunaikinimo, duomenų atkūrimas iš duomenų kopijų;	Informacinės sistemos administratorius
		9.1.4. jei nėra galimybių atkurti pakeistų ar sunaikintų duomenų iš duomenų kopijų, Informacinės sistemos duomenų gavėjų informavimas dėl būtinumo sugadintus ar prarastus duomenis iš naujo įrašyti į duomenų bazes.	Informacinės sistemos saugos įgaliotinis



**(Ministerijos informacinių sistemų veiklos testinumo valdymo plano bandymo ataskaitos
forma)**

**MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĖSTINUMO VALDYMO
EIGOS (PLANO BANDYMO) ATASKAITA**

(Veiklos testinumo valdymo grupės susitikimo data ir dokumento numeris)

Ekstremaliosios situacijos bandyme dalyvavo Veiklos testinumo valdymo grupės nariai:

1. _____
2. _____
3. _____
- ...

Ekstremaliosios situacijos apibūdinimas:

Informacinės sistemos, kurias paveikė ekstremalioji situacija:

Ekstremaliosios situacijos valdymo eiga:

Rasti Ministerijos informacinių sistemų veiklos testinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti Ministerijos informacinių sistemų veiklos testinumo valdymo
planą:

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)

(vardas, pavardė)

(parašas)

**ATSARGINIŲ PATALPŲ, NAUDOJAMŲ LIETUVOS RESPUBLIKOS APLINKOS
MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLAI ATKURTI, ĮVYKUS
ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTUI, ADRESAS IR, KAIP JAS
RASTI**

1. Atsarginių patalpų adresas: S. Konarskio g. 35, LT-03123 Vilnius, Lietuva
2. Atsarginių patalpų vieta žemėlapyje:

