

PATVIRTINTA

Lietuvos Respublikos aplinkos ministro
2011 m. d. įsakymu Nr.

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) reglamentuoja Ministerijos informacinių sistemų veiklos tęstinumo užtikrinimą. Plano reikalavimai yra privalomi visiems Ministerijos valstybės tarnautojams ir Darbuotojams dirbantiems pagal darbo sutartį (toliau – Darbuotojai). Planas įsigalioja nuo jo patvirtinimo dienos, vykdyti planą privaloma kilus ekstremaliosios situacijos grėsmei ir/ar paskelbus ekstremaliąją situaciją.

2. Plane vartojamos sąvokos:

Ekstremalioji situacija – dėl gamtos stichijos, gaisro, patalpų užliejimo, žemės drebėjimo, patalpų sugriuvimo ar netekimo, katastrofos, teroro išpuolio ar kitų neįvardintų force majeure sąlygų sutrikusi Informacinės sistemos veikla.

Veiklos tęstinumo valdymo grupė – nuolat veikianti grupė, užtikrinanti informacinės sistemos veiklos tęstinumui kylančių grėsmių valdymą ir informacinės sistemos atkūrimo koordinavimą esant ekstremaliajai situacijai.

Kitos Plane vartojamos sąvokos apibrėžtos Ministerijos informacinių sistemų duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos aplinkos ministro _____ įsakymu Nr._____, Lietuvos Respublikos įstatymuose, kituose teisės aktuose ir Lietuvos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

3. Planas parengtas vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), ir Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070).

4. Planui įgyvendinti nustatomos funkcijos ir įgaliojimai:

4.1. Ministerijos saugos įgaliotinis dalyvauja Veiklos tęstinumo valdymo grupėje ir teikia jai informaciją apie ekstremaliąją situaciją;

4.2. informacinių sistemų administratoriai užtikrina informacinių sistemų atkūrimą ir dalyvauja Veiklos atkūrimo grupės veikloje;

4.3. informacinių sistemų naudotojai privalo vykdyti Plano ir Veiklos tęstinumo valdymo grupės reikalavimus.

5. Finansinių ir kitų išteklių, numatomų Ministerijos informacinių sistemų veiklai atkurti, įvykus ekstremaliajai situacijai, šaltinius ir pobūdį numato ir pasirenka Veiklos tęstinumo valdymo grupė.

6. Ministerijos informacinių sistemų veikla laikoma atkurta, jeigu yra atkurtas ekstremaliosios situacijos metu sutrikęs prieinamumas, užtikrintas duomenų konfidencialumas ir vientisumas.

II. VEIKLOS VALDYMO IR ATKŪRIMO PRINCIPAI

7. Pagrindiniai ekstremaliųjų situacijų valdymo principai prioriteto tvarka yra šie:

7.1. Darbuotojų gyvybės ir sveikatos apsauga. Būtina užtikrinti visų Darbuotojų gyvybės ir sveikatos apsaugą, kol trunka ekstremalioji situacija ir likviduojami jos padariniai;

7.2. informacinių sistemų veiklos atkūrimas. Paskelbus ekstremaliąją situaciją, jei būtina, organizuojama informacinių sistemų fizinė sauga ir veiklos atkūrimas. Pirmiausia turi būti atkurtos kritiškiausios informacinių sistemų dalys ir užtikrintas jų prieinamumas;

7.3. Darbuotojų mokymas. Darbuotojai turi būti supažindinami su Ministerijos informacinių sistemų veiklos tęstinumo valdymo planu ir kitais teisės aktais, nustatančiais asmeninę kiekvieno Darbuotojo atsakomybę ekstremaliosios situacijos atveju;

7.4. 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.

8. Pagrindiniai informacinių sistemų, telekomunikacijų ir infrastruktūros atkūrimo principai yra šie:

8.1. informacinių sistemų ir joms veikti būtinų sistemų komponentų (infrastruktūros elementų) atkūrimo pirmumas. Pirmiausia būtina atkurti kritiškiausias Ministerijos veiklai vykdyti informacinių sistemų dalis;

8.2. būtino informacinių sistemų, jos komponentų, telekomunikacijų ir infrastruktūros rezervo užtikrinimas. Turi būti rezervuota minimaliai būtina įranga, reikalinga kritinių informacinių sistemų funkcijų vykdymui;

8.3. už informacinių sistemų, jų komponentų, telekomunikacijų ir infrastruktūros atkūrimą atsakingų Darbuotojų mokymai. Mokymai ir Plano bandymai turi būti organizuojami reguliariai. Esant Plano pakeitimų, atsakingi Darbuotojai turi būti nedelsiant su jais supažindinami.

III. EKSTREMALIOSIOS SITUACIJOS PASKELBIMAS

9. Ministerijos saugos įgaliotinis, gavęs informaciją apie galimą ekstremaliąją situaciją, organizuoja atsakingų už informacinių sistemų priežiūrą informacinių technologijų specialistų posėdį, skirtą informacijos apie galimą ekstremaliąją situaciją patikslinimui ir galimos žalos nustatymui. Posėdyje turi dalyvauti:

9.1. Ministerijos Informacinių technologijų skyriaus vedėjas;

9.2. Ministerijos saugos įgaliotinis.

10. Įvertinę situaciją, posėdžio dalyviai apie ją informuoja Veiklos tęstinumo valdymo grupės vadovą.

11. Jei nėra Darbuotojų, galinčių įvertinti situaciją, situaciją įvertina Veiklos tęstinumo valdymo grupės vadovas.

12. Ekstremaliąją situaciją savo potvarkiu gali skelbti tik Veiklos tęstinumo valdymo grupės vadovas.

13. Paskelbus ekstremaliąją situaciją, prireikus, Veiklos tęstinumo valdymo grupė turi parengti ir išplatinti informacinius pranešimus:

13.1. visiems Darbuotojams. Informaciniame pranešime turi būti pateikiamos rekomendacijos, kaip elgtis esant ekstremaliajai situacijai, nurodomi atsakingi Darbuotojai ir jų kontaktinė informacija;

13.2. informacinių sistemų duomenų gavėjams ir teikėjams;

13.3. viešosios informacijos skleidėjams;

13.4. teisės saugos institucijoms.

14. Ekstremaliąją situaciją gali atšaukti tik Veiklos tęstinumo valdymo grupės vadovas. Ekstremalioji situacija atšaukiama, kai:

14.1. priežastys, kurios sukėlė ekstremaliąją situaciją, išnyksta arba yra pašalinamos;

14.2. atkuriamas Ministerijos informacinių sistemų minimalus funkcionalumas, nustatytas detalioje informacijoje, būtinoje informacinių sistemų veiklai atkurti.

15. Atšaukus ekstremaliąją situaciją:

15.1. Ministerijos saugos įgaliotinis parengia Ministerijos informacinių sistemų veiklos tęstinumo valdymo eigos (plano bandymo) ataskaitą (2 priedas). Joje turi būti pateikiamos išvados ir pasiūlymai dėl Plano atnaujinimo. Ataskaitą tvirtina Veiklos tęstinumo valdymo grupės vadovas;

15.2. Veiklos tęstinumo valdymo grupė apie atšauktą ekstremaliąją situaciją prirėikus praneša Plano 13 punkte išvardytoms interesų grupėms.

IV. ORGANIZACINĖS NUOSTATOS

16. Veiklos atkūrimo grupė yra atskaitinga Veiklos tęstinumo valdymo grupei ir vykdo informacinių sistemų veiklos atkūrimą ir veikimo užtikrinimą esant ekstremaliajai situacijai.

17. Veiklos tęstinumo valdymo grupę sudaro:

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

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

17.3. Ministerijos Bendrųjų reikalų skyriaus vedėjas (Veiklos tęstinumo valdymo grupės vadovo pavaduotojas);

17.4. Ministerijos saugos įgaliotinis.

18. Veiklos tęstinumo valdymo grupės funkcijos:

18.1. skelbia (grupės vadovas) ekstremaliąją situaciją;

18.2. vykdo situacijos analizę ir priima sprendimus, susijusius su Ministerijos informacinių sistemų veiklos tęstinumo valdymo užtikrinimu;

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

18.4. pagal ekstremaliosios situacijos pobūdį sudaro Ministerijos Veiklos atkūrimo grupę;

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

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

18.7. bendrauja su teisėsaugos institucijomis;

18.8. organizuoja ir užtikrina fizinę saugą;

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

19. Veiklos atkūrimo grupę sudaro:

19.1. Ministerijos informacinių sistemų administratoriai;

19.2. kitų, Ministerijai pavaldžių, informacinių sistemų administratoriai (jei būtina);

19.3. išoriniai ekspertai (jei būtina).

20. Veiklos atkūrimo grupės funkcijos:

20.1. Ministerijos informacinių sistemų veiklos atkūrimas (iki minimalaus funkcionalumo, nustatytas detalioje informacijoje, būtinoje informacinių sistemų veiklai atkurti) ir jo priežiūra;

20.2. tarnybinių stočių veiklos atkūrimas ir jų priežiūra;

20.3. vidaus duomenų perdavimo tinklo veiklos atkūrimas ir jo priežiūra;

20.4. taikomųjų programų veiklos atkūrimas ir jų priežiūra;

20.5. informacinių sistemų naudotojų kompiuterių veiklos atkūrimas ir jų priežiūra;

20.6. kitos Veiklos tęstinumo valdymo grupės pavestos funkcijos.

21. Esant 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.).

22. Reaguojant į ekstremaliasias situacijas ir jas valdant, turi būti vadovaujamas principais, nurodytais Plano II skyriuje, ir veiksmais, išdėstytais Detaliojame ekstremaliosios situacijos valdymo ir informacinių sistemų veiklos atkūrimo plane (1 priedas).

23. Sprendimus dėl įrangos, reikalingos ekstremaliosios situacijos pasekmėms pakeisti, įsigijimo priima Veiklos testinumo valdymo grupė.

V. INFORMACIJA, BŪTINA INFORMACINIŲ SISTEMŲ VEIKLAI ATKURTI

24. Veiklos testinumo vykdymui užtikrinti turi būti surinkta ir naudojama detali informacija, būtina informacinių sistemų veiklai atkurti.

25. Detalios informacijos, būtinos veiklos testinimui, aprašo rengimą ir atnaujinimą organizuoja Ministerijos saugos įgaliotinis. Detalią informaciją sudaro:

25.1. informacinės sistemos ir jų neveikimo laikas. Pateikiama informacija apie informacinių sistemų poveikio Ministerijos veiklai vertinimo rezultatus: šių sistemų maksimalus neveikimo laikas ir jų veiklą palaikantys pagrindiniai komponentai;

25.2. esamos Informacinių sistemų techninės ir programinės įrangos sąrašai ir specifikacija;

25.3. minimaliai būtinos, informacinėms sistemoms atkurti skirtos įrangos specifikacija. Pateikiama informacija apie minimalią techninę ir programinę įrangą, kuri būtina informacinėms sistemoms atkurti;

25.4. Darbuotojų kompetencijos informacinėms sistemoms atkurti aprašymas;

25.5. kiekvieno Ministerijos pastato aukšto planai su laidų ir įrangos išdėstymo schemomis;

25.6. Ministerijos telekomunikacinių tinklų schemos;

25.7. kiekvienos informacinės sistemos ir jos duomenų atkūrimo metodas;

25.8. laikmenų su atsarginėmis duomenų kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

25.9. Ministerijos Darbuotojų sąrašas ir jų kontaktinė informacija;

25.10. įrangos įsigijimo ir jos priežiūros sutarčių sąvadas su kontaktine informacija;

25.11. kitos svarbios informacijos buvimo vieta.

26. Atsarginių patalpų, naudojamų veiklai atkurti, įvykus ekstremaliajai situacijai, reikalavimai:

26.1. pateikimas į patalpas turi būti registruojamas žurnale;

26.2. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

26.3. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės;

26.4. patalpose turi būti įrengtas rezervinis elektros energijos šaltinis, užtikrinantis įrangos veikimą ne trumpiau kaip 10 minučių;

26.5. patalpoje turi nuolat veikti oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema).

VI. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

27. Naudotojai turi būti pasirašytinai susipažinę su Planu.

28. Už Plano veiksmingumo išbandymą ir jo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą Veiklos testinumo valdymo grupės vadovui atsakingas Ministerijos saugos įgaliotinis.

29. Planas turi būti išbandomas esant esminių informacinių sistemų pokyčių, bet ne rečiau kaip kartą per dvejus metus. Plano bandymo metu Veiklos testinumo valdymo grupė išanalizuoja galimą (sumodeliuotą) ekstremaliąją situaciją, numato galimus jos valdymo būdus, galimus sprendimus ir parengia Plano bandymo ataskaitą pagal Ministerijos informacinių sistemų veiklos testinumo valdymo plano bandymo ataskaitos formą (2 priedas).

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

VII. BAIGIAMOSIOS NUOSTATOS

31. Naudotojai, pažeidę Plano ir kitų veiklos tęstinumą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

DETALUSIS EKSTREMALIOSIOS SITUACIJOS VALDymo IR INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO PLANAS

Situacija	Siūlomi veiksmai	Vykdytojai
Gautas pranešimas apie galimą ekstremaliąją situaciją	1. Pranešama Ministerijos Informacinių technologijų skyriaus vedėjui. 2. Surenkama informacija iš informacinių sistemų administratorių apie neveikiančias arba apgadintas informacines sistemas, patalpas arba patirtą kitokią žalą. 3. Pranešama Veiklos tęstinumo valdymo grupei.	Saugos įgaliotinis
	Skelbiama ekstremalioji situacija	Veiklos tęstinumo valdymo grupės vadovas
Nustatyta informacinėms sistemoms padaryta žala	1. Parengiamas priemonių planas kilusiam pavojui užkirsti, žalai likviduoti. 2. Sudaroma Veiklos atkūrimo grupė, atsižvelgiant į informacinių sistemų pažeidimus.	Veiklos tęstinumo valdymo grupė
Nustatytas patalpų pažeidimas ir (ar) pavojus Darbuotojų sveikatai arba gyvybei	1. Darbuotojai evakuojami iš darbo patalpų. 2. Pranešama atitinkamoms tarnyboms.	Veiklos tęstinumo valdymo grupė
Nustatyti informacinių sistemų pažeidimai, dėl kurių jos negali funkcionuoti	1. Priimamas sprendimas atkurti informacinę sistemą panaudojant rezervinę įrangą. 2. Organizuojamas pažeistų patalpų remontas, atstatymo darbai, komunalinių komunikacijų pajungimas.	Veiklos tęstinumo valdymo grupė
	Informacinių sistemų veiklos atkūrimas pasitelkus rezervinę įrangą.	Veiklos atkūrimo grupė
Nustatytas informacinių technologijų sistemų techninės, programinės įrangos ir (ar) duomenų praradimas	1. Parengiama atkūrimui būtina minimali techninė ir programinė įranga. 2. Atkuriamas informacinių sistemų techninės, programinės įrangos veikla. 3. Atkuriami prarasti duomenys.	Veiklos atkūrimo grupė
Nustatytas telekomunikacinių linijų sutrikimas, dėl kurio nustoja funkcionuoti informacinės sistemos	1. Nustatomos telekomunikacijų sutrikimo priežastys. 2. Šalinami telekomunikacijų sutrikimai šalinimas arba telekomunikacijų paslaugų tiekėjas užklauiamas dėl įvykusio sutrikimo pašalinimo trukmės prognozės. 3. Aktyvuojamos rezervinės telekomunikacinės priemonės.	Veiklos atkūrimo grupė

Situacija	Siūlomi veiksmai	Vykdytojai
	Pranešama atitinkamų tarnybų ir duomenų gavėjams.	Veiklos tęstinumo valdymo grupė
Nustatytas techninės įrangos sugadinimas, dėl kurio nustoja funkcionuoti informacinės sistemos	1. Priimamas sprendimas dėl techninės įrangos perskirstymo. 2. Prireikus kreipiamasi į techninės įrangos tiekėjus dėl sugadintos įrangos remonto, nuomos ar naujos techninės įrangos įsigijimo.	Veiklos tęstinumo valdymo grupė
	Perskirstoma esama techninė įranga ir kiti ištekliai, reikalingi Ministerijos informacinių sistemų veiklai užtikrinti.	Veiklos atkūrimo grupė
Nustatytas programinės įrangos sugadinimas, dėl kurio nustoja funkcionuoti informacinės sistemos	Priimamas sprendimas dėl programinės įrangos įsigijimo.	Veiklos tęstinumo valdymo grupė
	Iš esamų arba įsigytų programinės įrangos kopijų atkuriamas sugadinta ar prarasta programinė įranga..	Veiklos atkūrimo grupė
Nustatytas duomenų sugadinimas ar praradimas, dėl kurio nustoja funkcionuoti informacinės sistemos.	1. Atkuriami prarasti duomenys. 2. Nepasisekus visiškai atkurti sugadintų ar prarastų duomenų iš atsarginių duomenų kopijų, Veiklos atkūrimo grupė organizuoja trūkstamų duomenų įkėlimą iš naujo.	Veiklos atkūrimo grupė

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

**MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TESTINUMO 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)