PATVIRTINTA
Lietuvos Respublikos aplinkos ministro
2010 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 ir galioja šioms informacinėms sistemoms: Aplinkos informacijos valdymo integruota kompiuterinė sistema, Aplinkosaugos leidimų informacinė sistema, Intelektuali miškų ūkio elektroninių paslaugų informacinė sistema, Saugomų rūšių informacinė sistema (toliau – informacinės sistemos). Plano reikalavimai yra privalomi visiems Naudotojams. Planu vadovaujamasi kilus ekstremaliosios situacijos grėsmei ir/ar paskelbus ekstremaliąją situaciją.

2. Plane vartojamos sąvokos:

Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

Ekstremalioji situacija – situacija, kuri skelbiama įvykus elektroninės informacijos saugos incidentui, kuris sutrikdo ar pakeičia informacinių sistemų veiklą, kai informacinėmis sistemomis nebegali naudotis Naudotojai.

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. Planas įsigalioja nuo jo patvirtinimo dienos.

5. Planui įgyvendinti nustatomos funkcijos ir įgaliojimai:

5.1. Saugos įgaliotinis dalyvauja Veiklos tęstinumo valdymo grupėje ir teikia jai informaciją apie elektroninės informacijos saugos incidentus;

5.2. administratorius užtikrina informacinių sistemų atkūrimą ir dalyvauja Veiklos atkūrimo grupės veikloje;

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

6. Finansinių ir kitų išteklių, numatomų Ministerijos informacinių sistemų veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, šaltinius ir pobūdį numato ir pasirenka Veiklos tęstinumo valdymo grupė.

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

II. ORGANIZACINĖS NUOSTATOS

8. Veiklos atkūrimo grupė yra atskaitinga Veiklos tęstinumo valdymo grupei ir vykdo informacinių sistemų veiklos atkūrimą ir veikimo užtikrinimą įvykus elektroninės informacijos saugos incidentui.

9. Veiklos tęstinumo valdymo grupę sudaro:

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

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

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

9.4. Saugos įgaliotinis.

10. Veiklos tęstinumo valdymo grupės funkcijos:

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

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

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

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

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

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

10.7. bendrauja su teisėsaugos institucijomis;

10.8. organizuoja ir užtikrina fizinę saugą;

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

11. Veiklos atkūrimo grupę sudaro:

11.1. Ministerijos Informacinių technologijų skyriaus vedėjas (Atkūrimo grupės vadovas);

11.2. Ministerijos Informacinių technologijų skyriaus vyr. specialistas (Atkūrimo grupės vadovo pavaduotojas);

11.3. Ministerijos Bendrųjų reikalų skyriaus vedėjas (Atkūrimo grupės vadovo pavaduotojas);

11.4. Urėdijos saugos įgaliotinis;

11.5. Agentūros saugos įgaliotinis;

11.6. Administratorius;

11.7. kitų, Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai;

11.8. išoriniai ekspertai (jei būtina).

12. Veiklos atkūrimo grupės funkcijos:

12.1. Ministerijos informacinių sistemų veiklos atkūrimas (iki minimalaus funkcionalumo, nustatytas detalioje informacijoje, būtinoje informacinių sistemų veiklai atkurti) ir jų priežiūra (Administratorius ir Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai);

12.2. tarnybinių stočių veiklos atkūrimas ir jų priežiūra (Administratorius ir Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai);

12.3. vidaus duomenų perdavimo tinklo veiklos atkūrimas ir jo priežiūra Administratorius ir Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai);

12.4. taikomųjų programų veiklos atkūrimas ir jų priežiūra (Administratorius ir Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai);

12.5. informacinių sistemų naudotojų kompiuterių veiklos atkūrimas ir jų priežiūra (Administratorius ir Ministerijai pavaldžių įstaigų, informacinių sistemų administratoriai);

12.6. kitos Veiklos tęstinumo valdymo grupės pavestos funkcijos.

13. 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.).

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

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

14.2. informacinių sistemų veiklos atkūrimas. Paskelbus ekstremaliąją situaciją, jei būtina, organizuojama fizinė sauga ir veiklos atkūrimas. Pirmiausia atkuriamos kritiškiausios informacinės sistemos ir užtikrintas jų prieinamumas;

14.3. darbuotojų mokymas. Darbuotojai, dirbantys su informacinių sistemų, turi būti supažindinti su Planu ir kitais teisės aktais, nustatančiais asmeninę kiekvieno darbuotojo atsakomybę ekstremaliosios situacijos atveju;

14.4. 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.

15. Per ekstremalią situaciją sunaikinta techninė, sisteminė ir taikomoji programinė įranga keičiame turima rezervine arba testine informacinių sistemų aplinkos įranga, vėliau įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo (Žin., 1996, Nr. 84-2000; 2006, Nr. 4-102) nustatyta tvarka, įsigijimo ištekliai padengiami iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių.

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

16.1. patekimas į patalpas turi būti registruojamas žurnale;

16.2. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

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

16.4. 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;

16.5. ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo;

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

III. APRAŠOMOSIOS NUOSTATOS

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

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

18.1. 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;

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

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

18.4. Darbuotojų kompetencijos informacinėms sistemoms atkurti aprašymas;

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

18.6. Ministerijos telekomunikacinių tinklų schemos;

18.7. kiekvienos informacinės sistemos ir jos duomenų atkūrimo metodas;

18.8. kiekvieno pastato patalpų brėžiniai ir šiose patalpose esančios įrangos bei komunikacijų sąrašas;

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

18.10. Ministerijos Darbuotojų sąrašas ir jų kontaktinė informacija;

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

18.12. kitos svarbios informacijos buvimo vieta.

19. Atsarginių patalpų, naudojamų informacinių sistemai veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, adresas ir, kaip jas rasti, nurodyta 3 priede.

IV. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

20. Naudotojai turi būti pasirašytinai susipažinę su Planu.

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

22. Planas turi būti išbandomas esant esminių informacinių sistemų pokyčių, 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).

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

V. BAIGIAMOSIOS NUOSTATOS

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

_____

Lietuvos Respublikos aplinkos ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
1 priedas

DETALUSIS EKSTREMALIOSIOS SITUACIJOS VALDYMO IR INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO PLANAS

Situacija	Siūlomi veiksmai	Vykdytojai
Gautas pranešimas apie elektroninės informacijos saugos incidentą	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
	Prireikus parengiami ir išplatinami informaciniai pranešimai interesų grupėms: • visiems Ministerijos darbuotojams. Informaciniame pranešime turi būti pateikiamos rekomendacijos, kaip elgtis esant ekstremaliai situacijai, nurodomi atsakingi darbuotojai ir jų kontaktinė informacija; • informacinių sistemų duomenų gavėjams ir teikėjams; • viešosios informacijos skleidėjams; • teisėsaugos institucijoms.	Veiklos tęstinumo valdymo grupė
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	1. Parengiama atkūrimui būtina minimali techninė	Veiklos atkūrimo

Situacija	Siūlomi veiksmai	Vykdytojai
informacinių technologijų sistemų techninės, programinės įrangos ir (ar) duomenų praradimas	ir programinė įranga.2. Atkuriama informacinių sistemų techninės, programinės įrangos veikla. 3. Atkuriami prarasti duomenys.	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 užklausiamas dėl įvykusio sutrikimo pašalinimo trukmės prognozės. 3. Aktyvuojamos rezervinės telekomunikacinės priemonės.	Veiklos atkūrimo grupė
	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 atkuriama 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
Priežastys, kurios sukėlė ekstremaliąją situaciją, išnyksta ar yra pašalinamos, arba atkuriamas informacinių sistemų minimalus funkcionalumas.	Atšaukiama ekstremali situacija	Veiklos tęstinumo valdymo grupės vadovas
	Užpildoma Ministerijos informacinių sistemų veiklos tęstinumo valdymo eigos (plano bandymo) ataskaita (2 priedas).	Administratorius
	Apie atšauktą ekstremalią situaciją prireikus pranešama interesų grupėms.	Veiklos atkūrimo grupė

_____

Lietuvos Respublikos aplinkos ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
2 priedas

(Ministerijos informacinių sistemų veiklos tęstinumo valdymo plano bandymo ataskaitos forma)

MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO EIGOS (PLANO BANDYMO) ATASKAITA

(Veiklos tęstinumo valdymo grupės susitikimo data ir dokumento numeris)

Ekstremaliosios situacijos bandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai:

1.

2.

3.

...

Ekstremaliosios situacijos apibūdinimas:

Informacinės sistemos, kurias paveikė ekstremalioji situacija:

Ekstremaliosios situacijos valdymo eiga:

Rasti Ministerijos informacinių sistemų veiklos tęstinumo valdymo plano trūkumai:

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

(vardas, pavardė)	(parašas)
(vardas, pavardė)	(parašas)
(vardas, pavardė)	(parašas)

Lietuvos Respublikos aplinkos ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
3 priedas

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 35, LT-03123 Vilnius, Lietuva
2. Atsarginių patalpų vieta žemėlapyje: