PATVIRTINTA
Lietuvos dailės muziejaus
direktoriaus
2010 m. kovo 1 d.
įsakymu Nr. V-1-29

LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS (LIMIS) VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (LIMIS) veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja LIMIS veiklos tęstinumo užtikrinimą, o jo reikalavimai privalomi visiems LIMIS naudotojams.

2. LIMIS veiklos tęstinumo valdymo planas pagrįstas šiais principais:

2.1. LIMIS naudotojų gyvybės ir sveikatos apsauga (būtina užtikrinti visų informacinės sistemos naudotojų gyvybės ir sveikatos apsaugą bei saugumą, kol trunka elektroninės informacijos saugos incidentas ir yra likviduojami avarijų padariniai);

2.2. LIMIS veiklos atkūrimas (atkuriama pagal šiame plane numatytą posistemių prioritetą (l priedas); atsakingų asmenų funkcijos ir veiksmai aprašyti LIMIS veiklos tęstinumo detaliajame plane (2 priedas);

2.3. LIMIS naudotojų mokymas (LIMIS naudotojai pasirašytinai supažindinami su planu ir teisės aktais, nustatančiais kiekvieno informacinės sistemos naudotojo atsakomybę).

3. Šis planas įsigalioja esant elektroninės informacijos saugos incidentui – veiksmams ir (ar) aplinkybėms (pvz., gamtos veiksniai, gaisro, įrangos gedimo), keliantiems pavojų LIMIS naudotojų gyvybei ar sveikatai, dėl kurių Lietuvos dailės muziejaus filialas Lietuvos muziejų informacijos, skaitmeninimo ir LIMIS centras (toliau – LIMIS centras) gali prarasti arba prarado kompiuterinę įrangą ir (arba) duomenis, reikalingus LIMIS funkcijoms vykdyti.

4. LIMIS veiklos tęstinumo valdymo plane naudojamos LIMIS nuostatuose ir LIMIS duomenų saugos nuostatuose apibrėžtos sąvokos ir trumpinimai.

5. Šis 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 „Dėl duomenų saugos valstybės institucijų ir įstaigų informacinėse sistemose“ (Žin., 1997, Nr. 83-2075; 2003, Nr. 2-45, 2007, Nr. 49-1891), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. lV-172 (Žin., 2007, Nr. 53-2070), LIMIS duomenų saugos nuostatais, patvirtintais LDM direktoriaus 2010 m.

vasario 26 d. įsakymu Nr. V.1-26 „Dėl Lietuvos integralios muziejų informacinės sistemos Duomenų saugos nuostatų patvirtinimo, duomenų [...]“.

6. Už Plano įgyvendinimą atsakingos LIMIS tvarkymo įstaigos, Lietuvos dailės muziejus ir jų LIMIS duomenis tvarkyti paskirti fiziniai asmenys – LM tvarkytojai, LIMIS-C administratorius.

7. Už Plano įgyvendinimo organizavimą ir kontrolę atsakingas LIMIS saugos įgaliotinis.

8. LIMIS tvarkymo įstaigų ir Lietuvos dailės muziejaus LIMIS duomenis tvarkyti paskirtų fizinių asmenų – LM tvarkytojų, LIMIS-C administratoriaus, LIMIS saugos įgaliotinio – funkcijos ir veiksmai elektroninės informacijos saugos incidento metu nurodyti LIMIS veiklos tęstinumo detaliajame plane (1 priedas).

9. Informacijos saugos incidentų, įvykusių LIMIS, tyrimas LIMIS centre vyksta pagal nustatytą tvarką (3 priedas).

10. LIMIS veiklos atkūrimas finansuojamas iš Lietuvos Respublikos valstybės biudžeto ir kitų teisės aktuose nustatytų finansavimo šaltinių.

11. LIMIS elektroninės informacijos prieinamumas užtikrinamas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis. Kriterijai, pagal kuriuos nustatoma, kad LIMIS veikla atkurta, yra:

11.1. nuolat atnaujinami LIMIS duomenys;

11.2. išsaugomi atnaujinti LIMIS duomenys;

11.3. LIMIS duomenys teikiami vešiesiems katalogams;

11.4. vykdomas LIMIS duomenų rezervinis kopijavimas.

12. Reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti elektroninės informacijos saugos incidento atveju, aprašyti 4 priede.

II. ORGANIZACINĖS NUOSTATOS

13. Elektroninės informacijos saugos incidentams valdyti bei veiklos atstatymui organizuoti LDM direktoriaus įsakymu tvirtinamos 2 grupės: Informacinės sistemos veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir Veiklos atkūrimo grupė (toliau – Atkūrimo grupė).

14. Valdymo grupės tikslai – tirti elektroninės informacijos saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams bei žalai likviduoti, užtikrinti LIMIS veiklos tęstinumą. Valdymo grupę sudaro:

14.1. Valdymo grupės vadovas – duomenų saugos įgaliotinis;

14.2. Valdymo grupės vadovo pavaduotojai: LIMIS centro vedėjas, LIMIS centro Informacinių technologijų ir LIMIS skyriaus vedėjas, LDM Informacinių sistemų tarnybos vedėjas;

14.3. Valdymo grupės nariai: LDM Pastatų ir techninių įrenginių eksploatavimo tarnybos vyresnysis inžinierius, LDM vyriausioji buhalterė, LDM direktoriaus pavaduotojas ūkiui, LDM Personalo skyriaus vedėjas. Sekretorius strateginiam planavimui grupės veikloje gali dalyvauti stebėtojo teisėmis.

15. Valdymo grupės funkcijos, užtikrinant veiklos tęstinumą:

15.1. situacijos analizė, problemų (incidentų) nustatymas;

15.2. sprendimų informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas ir kontrolė;

15.3. bendravimas su teisėsaugos ir kitomis institucijomis, LIMIS naudotojų informavimas;

15.4. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, nustatymas ir naudojimo kontrolė;

15.5. elektroninės informacijos fizinės saugos, įvykus elektroninės informacijos saugos incidentui, užtikrinimas;

15.6. logistika (žmonių, daiktų, įrangos gabenimas) ir jos organizavimas;

15.7. bendravimas su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis, žiniasklaidos atstovais;

15.8. kitos pavestos funkcijos.

16. Atkūrimo grupę sudaro: vadovas – duomenų saugos įgaliotinis; pavaduotojai – LIMIS centro vedėjas, LIMIS centro Informacinių technologijų ir LIMIS skyriaus vedėjas; nariai – LDM Informacinių sistemų tarnybos, LIMIS centro Informacinių technologijų ir LIMIS skyriaus specialistai.

17. Veiksmai, įvykus esminiams pokyčiams informacinėje sistemoje:

17.1. informacinės sistemos ir jos duomenų atkūrimo organizavimas;

17.2. tarnybinių stočių veikimo atkūrimo organizavimas;

17.3. kompiuterių tinklo veikimo atkūrimo organizavimas;

17.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

17.5. kompiuterizuotų darbo vietų veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

17.6. informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

17.7. kitų atkūrimo grupei pavestų funkcijų vykdymas.

18. Įvykus elektroninės informacijos saugos incidentui LIMIS centro patalpose, kuriose yra LIMIS tarnybinės stoties administravimo techninė ir programine įranga:

18.1. LIMIS-C administratorius nedelsdamas informuoja apie elektroninės informacijos saugos incidentą LIMIS saugos įgaliotinį ir LIMIS centro vedėją;

18.2. LIMIS centro vedėjas apie elektroninės informacijos saugos incidentą nedelsdamas informuoja LDM direktorių;

18.3. LIMIS-C administratorius atkuria LIMIS tarnybinės stoties, kompiuterių tinklo veiklą, LIMIS duomenis, LIMIS techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai nedelsdamas informuoja LIMIS centro vedėją ir LIMIS saugos įgaliotinį;

18.4. LIMIS saugos įgaliotinis organizuoja žalos LIMIS duomenims, LIMIS techninei, programinei įrangai vertinimą, koordinuoja LIMIS veiklai atkurti techninės, sisteminės ir taikomosios programinės įrangos įsigijimą;

18.5. Saugos įgaliotinis, vadovaudamasis valdymo planu, užtikrina LIMIS veiklos atkūrimą per 8 valandas.

19. Valdymo grupė organizuoja susirinkimą kartą per metus arba įvykus esminiams pokyčiams.

20. Atkūrimo grupės pasitarimai organizuojami įvykus elektroninės informacijos saugos incidentui.

21. Valdymo grupė ir Atkūrimo grupė bendravimui naudoja elektroninio pašto bei telefono ryšio priemones.

22. Nauja įranga vietoje elektroninės informacijos saugos incidento metu sunaikintos ar sugadintos įrangos įsigyjama viešųjų pirkimų būdu.

23. Įvykus elektroninės informacijos saugos incidentui LIMIS centre, LIMIS veiklai atkurti naudojamos atsarginės patalpos. Reikalavimai LIMIS veiklai atkurti elektroninės informacijos saugos incidento atveju naudojamoms atsarginėms patalpoms ir patalpų adresas aprašyti 4 priede.

III. APRAŠOMOSIOS NUOSTATOS

24. LIMIS centro Informacinių technologijų ir LIMIS skyriuje saugoma:

24.1. Informacinių technologijų (IT) įrangos sąrašas;

24.2. Kompiuterizuotų darbo vietų (KDV) kortelės, kuriose aprašyti IT įrangos parametrai (už šios įrangos priežiūrą, KDV apskaitą atsakingas LIMIS-C administratorius);

24.3. tarnybinių stočių išdėstymo schema, kompiuterių tinklo fizinio ir loginio sujungimo schemos, techninės ir programinės įrangos priežiūros sutarčių sąrašas.

25. LIMIS tarnybinės stoties administravimo, LIMIS techninės ir programinės įrangos sąrašai, LIMIS specifikacija saugoma LIMIS centre.

26. LIMIS duomenų, LIMIS programinės įrangos sukūrimo, modernizavimo, priežiūros, kitų paslaugų teikimo sutartys saugomos LIMIS centre.

27. LIMIS atsarginių duomenų kopijos daromos LDM direktoriaus patvirtintame LIMIS atsarginių duomenų kopijų darymo apraše nurodyta tvarka.

28. Už LIMIS atsarginių duomenų kopijų darymą, saugojimą, duomenų iš LIMIS

atsarginių duomenų kopijų atkūrimą atsako LIMIS-C administratorius.

29. Nesant LIMIS-C administratoriaus, sistemos veiklą elektroninės informacijos saugos incidento metu organizuoja įmonė pagal paslaugų teikimo sutartyje numatytus atlikti darbus ir įkainius.

30. LDM Personalo skyriuje saugomi visų LDM darbuotojų darbo telefonų numeriai, o Valdymo bei Atkūrimo grupių narių – papildomai dar ir mobiliojo bei namų telefono numeriai, el. pašto ir gyvenamosios vietos adresai.

IV. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

31. Saugos įgaliotinis organizuoja LIMIS naudotojų supažindinimą su šiuo planu.

32. LIMIS saugos įgaliotinis, per kalendorinius metus įvertinęs rizikos veiksnių galimybes ne mažiau kaip šešiose LIMIS tvarkymo įstaigose, išnagrinėjęs įrašus LIMIS elektroninės informacijos saugos incidentų registravimo žurnale (6 priedas), du kartus per metus (pirmo pusmečio – iki liepos mėnesio 10 dienos, antro pusmečio – iki kitų metų sausio mėnesio 10 dienos) – parengia LIMIS rizikos įvertinimo ataskaitą (toliau – Ataskaita) (5 priedas). Ataskaitą tvirtina LDM direktorius.

33. LIMIS saugos įgaliotinis patvirtintos Ataskaitos kopiją el. paštu siunčia LIMIS tvarkymo įstaigoms, nuolat kontroliuoja Ataskaitoje nurodytų prevencinių priemonių įgyvendinimą.

34. Plano veiksmingumo išbandymo data nustatoma kiekvienais metais sausio mėnesį. Nustatytą dieną imituojami elektroninės informacijos saugos incidentai, jų metu atsakingi pasekmių likvidavimo vykdytojai atlieka elektroninės informacijos saugos incidento metu būtinus atlikti veiksmus. Atsarginėje LIMIS tarnybinėje stotyje iš atsarginių LIMIS duomenų kopijose esamų duomenų atkuriami LIMIS duomenys.

35. LIMIS saugos įgaliotinis atsakingas už išbandymo metu pastebėtų Plano veiksmingumo trūkumų parengimą ir pateikimą LDM direktoriui.

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

_____

SUDERINTA
Vidaus reikalų ministerijos
2010 m. vasario 25 d. raštu Nr. 1D-1387 (6)

LIMIS veiklos tęstinumo
valdymo plano
1 priedas

LIMIS ATKŪRIMO PRIORITETAI IR ATSAKOMYBĖ

Eil. Nr.	**Aprašymas**	**Atsakingas už atkūrimą**
1.	Kompiuterių tinklo veikimo atkūrimo organizavimas	LIMIS-C administratorius
2.	Tarnybinių stočių veikimo atkūrimo organizavimas	LIMIS-C administratorius
3.	Kompiuterizuotų darbo vietų veikimo atkūrimo organizavimas	LIMIS-C administratorius
4.	LIMIS-C posistemis	LIMIS-C administratorius
5.	LIMIS-K posistemis	LIMIS-C administratorius
6.	LIMIS-M posistemis	LM tvarkytojai

_____

LIMIS veiklos tęstinumo
valdymo plano
2 priedas

LIMIS VEIKLOS TĘSTINUMO DETALUSIS PLANAS

Eil. Nr.	Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi vykdytojai
1.	Gamtos reiškiniai (potvynio, uragano, oro ir kt. pavojus)	1.1. Elektroninės informacijos saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas.	1.1.1. elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			1.1.2. priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas.	Duomenų saugos įgaliotinis
			1.1.3. darbuotojų informavimas, padarytą žalą likviduojančių darbuotojų instruktavimas.	Duomenų saugos įgaliotinis
			1.1.4. elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas, pirmosios pagalbos suteikimas nukentėjusiems darbuotojams.	LIMIS-C administratorius
2.	Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas.	2.1.1. įvykio vietos lokalizavimas, jei yra rekomendacija iš Priešgaisrinės gelbėjimo tarnybos.	Duomenų saugos įgaliotinis
		2.2. Gaisro gesinimas anksty-voje stadijoje, jei yra rekomen-dacija dirbti pavojaus zonoje.	2.1.2. galimybių evakuoti darbuotojus nagrinėjimas, jei yra rekomendacija iš Priešgaisrinės gelbėjimo tarnybos.	Duomenų saugos įgaliotinis
		2.3. Darbas pavojaus zonoje: komunikacijų, sukeliančių pavojų, išjungimas.	2.1.3. darbuotojų informavimas apie evakavimą, jei yra rekomendacija.	Duomenų saugos įgaliotinis
			2.1.4. darbuotojų informavimas apie saugų darbą pavojaus zonoje.	Duomenų saugos įgaliotinis
			2.1.5. elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			2.1.6. padarytą žalą likviduojančių darbuotojų instruktavimas.	Duomenų saugos įgaliotinis

			2.1.7. elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas.	LIMIS-C administratorius
3.	Elektros energijos tiekimo sutrikimai	3.1. Energijos tiekimo sutrikimo priežasčių nustatymas.	3.1.1. rekomendacijų iš energijos tiekimo tarnybos gavimas.	LIMIS-C administratorius
		3.2. Tarnybinių stočių, kitos techninės įrangos energijos maitinimo išjungimas.	3.1.2. padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
		3.3. Kreipimasis į energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių.	3.1.3. žalą likviduojančių darbuotojų instruktavimas.	Duomenų saugos įgaliotinis
		3.4. Sutrikimų pašalinimas.	3.1.4. padarytos žalos likvidavimas.	LIMIS-C administratorius
4.	Vandentiekio ir šildymo sistemų sutrikimai	4.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas.	4.1.1. paslaugų teikėjų rekomendacijų gavimas.	LIMIS-C administratorius
			4.1.2. darbuotojų informavimas apie rekomendacijas.	Duomenų saugos įgaliotinis
		4.2. Sutrikimo šalinimo prognozės skelbimas.	4.2.1. padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			4.2.2. padarytos žalos likvidavimas.	LIMIS-C administratorius
5.	Ryšio sutrikimas	5.1. Ryšio sutrikimo priežasčių nustatymas.	5.1.1. ryšio paslaugos teikėjo rekomendacijų gavimas.	LIMIS-C administratorius
		5.2. Ryšio tarnybų informavimas, sutrikimo trukmės ir šalinimo prognozės.	5.1.2. sutrikimo likvidavimas. Nustatyti ir įgyvendinti priemones, kad sutrikimai nesikartotų.	LIMIS-C administratorius
6.	Įsilaužimas į vidinį kompiuterių tinklą	6.1. Pranešti teisėsaugos tarnybai apie įvykį.	6.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis, LIMIS-C administratorius
		6.2. Priemonių plano sudarymas ir įgyvendinimas.	6.1.2. elektroninės informacijos saugos incidento pasekmės likvidavimas.	LIMIS-C administratorius
7.	Pagrindinių tarnybinių stočių sugadinimas ir / arba praradimas	7.1. Pranešti teisėsaugos tarnybai apie įvykį.	7.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis, LIMIS-C administratorius
		7.2. Priemonių plano sudarymas ir įgyvendinimas.	7.1.2. padarytą žalą likviduojančių darbuotojų instruktavimas.	Duomenų saugos įgaliotinis
			7.1.3. elektroninės informacijos saugos incidento pasekmės likvidavimas.	LIMIS-C administratorius
			7.1.4. padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			7.1.5. žalos padarinių likvidavimas.	LIMIS-C administratorius

8.	Vagystė iš duomenų bazės ar jos fizinis sunaikinimas	8.1. Pranešti teisėsaugos tarnybai apie įvykį.	8.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis
		8.2. Priemonių plano sudarymas ir įgyvendinimas.	8.1.2. padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis, LIMIS-C administratorius
			8.1.3. duomenų atkūrimas iš atsarginių kopijų.	LIMIS-C administratorius
9.	Programinės įrangos sugadinimas, praradimas	9.1. Pranešti teisėsaugos tarnybai apie įvykį.	9.1.1. teisėsaugos tarnybos nurodymų vykdymas, priemonių plano sudarymas ir įgyvendinimas.	Duomenų saugos įgaliotinis
		9.2. Programinės įrangos kopijų periodinis gaminimas.	9.1.2. elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			9.1.3. žalą likviduojančių darbuotojų instruktavimas.	Duomenų saugos įgaliotinis
			9.1.4. padarytos žalos likvidavimas.	LIMIS-C administratorius
10.	Vagystė.	10.1. Pranešti teisėsaugos tarnybai apie įvykį.	10.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis
		10.2. Priemonių plano sudarymas ir įgyvendinimas.	10.1.2. vagystės metu padarytos žalos įvertinimas.	Duomenų saugos įgaliotinis
			10.1.3. vagystės padarinių likvidavimas.	LIMIS-C administratorius
11.	Pavojingas (įtartinas) radinys	11.1. Pranešti teisėsaugos tarnybai apie įvykį.	11.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis
12.	Įvykis susijęs su teroristine veikla	12.1. Pranešti teisėsaugos tarnybai apie įvykį.	12.1.1. teisėsaugos tarnybos nurodymų vykdymas.	Duomenų saugos įgaliotinis
		12.2. Darbuotojų evakavimas, jei yra rekomendacija.	12.1.2. darbuotojų informavimas apie nurodymų vykdymą.	Duomenų saugos įgaliotinis
13.	Dokumentų praradimas	13.1. Vadovybės informavimas.	13.1.1. prarastų dokumentų gavimas.	Duomenų saugos įgaliotinis

14.	Darbuotojų praradimas	14.1. elektroninės informacijos saugos incidento pasekmės įvertinimas.	14.1.1. trūkstamų darbuotojų paieška ir priėmimas į darbą.	Duomenų saugos įgaliotinis

LIMIS veiklos tęstinumo
valdymo plano
3 priedas

LIMIS SAUGOS INCIDENTŲ TYRIMO TVARKA

1. Apie įvykusį elektroninės informacijos saugos incidentą LIMIS naudotojai privalo nedelsdami žodžiu ar raštu pranešti LIMIS-C administratoriui. Patys LIMIS naudotojai neturi teisės imtis jokių atsakomųjų veiksmų.

2. LIMIS-C administratorius nedelsiant turi imtis adekvačių atsakomųjų veiksmų, reikalingų elektroninės informacijos saugos incidentui stabdyti, apie jį pranešdamas duomenų saugos įgaliotiniui. Duomenų saugos įgaliotinis, kartu su kitais Atkūrimo grupės nariais įvertinęs incidento reikšmingumą, aprašo įvykį raštu, nurodydamas incidento vietą, laiką, ir pateikia kitą su įvykiu susijusią informaciją.

3. Duomenų saugos įgaliotinis organizuoja tolimesnius darbus, remdamasis „LIMIS veiklos tęstinumo detaliuoju planu“, ir pateikia LDM direktoriui tarnybinį pranešimą apie saugos incidentą.

4. LIMIS-C administratorius atitinkamai pagal patvirtintą savo atsakomybės sritį surenka visą su incidentu susijusią informaciją ir ją dokumentuoja, registruoja informacinės sistemos atkuriamuosius darbus elektroninės informacijos saugos incidentų registravimo žurnale.

5. Elektroninės informacijos saugumo incidentui peržengus LIMIS centro ribas, duomenų saugos įgaliotinis informuoja su incidentu susijusius paslaugų teikėjus ir / ar kitas institucijas, atsižvelgia į jų rekomendacijas ir vykdo jų nurodymus.

_____

LIMIS veiklos tęstinumo
valdymo plano
4 priedas

REIKALAVIMAI, KELIAMI ATSARGINĖMS PATALPOMS, NAUDOJAMOMS LIMIS VEIKLAI ATKURTI ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTO ATVEJU

1. Patalpos atskirtos nuo bendrojo naudojimo patalpų.

2. Patalpose įrengta langų ir durų fizinė apsauga. Languose įrengtos žaliuzės, durys rakinamos, veikia durų signalizacija.

3. Patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės.

4. Ryšių kabeliai apsaugomi nuo neteisėto prisijungimo prie jų ir pažeidimo.

5. Įgyvendintos gamintojo nustatytos techninės įrangos eksploatavimo sąlygos.

6. Patalpoje yra elektros energijos įvadas.

7. Patalpoje yra saugaus valstybinio duomenų perdavimo tinklo (SVDPT) įvadas.

8. Patalpos įrengiamos Lietuvos dailės muziejaus patalpose Bokšto g. 5, Vilniuje.

_____

LIMIS veiklos tęstinumo
valdymo plano
5 priedas

INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO BANDYMO ATASKAITA

(Grupės susitikimo data ir dokumento numeris)

Elektroninės informacijos saugos incidento bandyme dalyvavo Grupės nariai:

1. _____
2. _____
3. _____
4. _____
5. _____

Elektroninės informacijos saugos incidento scenarijus:

Informacinės sistemos, kurias paveikia elektroninės informacijos saugos incidentas:

Elektroninės informacijos saugos incidento pašalinimo eiga:

Rasti elektroninės informacijos saugos incidento valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti elektroninės informacijos saugos incidentų valdymo planą:

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

_____

(vardas, pavardė) (parašas)

LIMIS veiklos tęstinumo
valdymo plano
6 priedas

LIMIS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 201_m. _____ mėn. ___ d.

Eil. Nr.	Elektroninės informacijos saugos incidentas						
	Registro tvarkymo įstaigos pavadinimas	Požymio kodas	Įvykio aprašymas	Pradžia *(*metai, mėnuo, diena, valanda*)*	Pabaiga (metai, mėnuo, diena, valanda*)*	Pašalino (vardas, pavardė)	Registro saugos įgaliotinis (vardas, pavardė, parašas)
1							
2							
3							
4							
5							
6							

Elektroninės informacijos saugos incidento požymiai:

1. oro sąlygos; 2. gaisras; 3. patalpų užgrobimas; 4. patalpų pažeidimas arba praradimas; 5. energijos tiekimo sutrikimai; 6. vandentiekio ir šildymo sistemos sutrikimai; 7. ryšio sutrikimai; 8. tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas;
9. programinės įrangos sugadinimas, praradimas; 10. duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas; 11. darbuotojų praradimas.