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

LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS (LIMIS) SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (LIMIS) Saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, pagal kurią turi būti saugiai tvarkoma LIMIS informacinėje sistemoje esanti elektroninė informacija.

2. Taisyklės yra privalomos LIMIS-C administratoriui ir LIMIS naudotojams. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas saugos įgaliotinis.

3. Šios Taisyklės parengtos 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 apsaugos 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. 1V-172 (Žin., 2007, Nr. 53-2070), LIMIS duomenų saugos nuostatais, Lietuvos dailės muziejaus direktoriaus 2010 m. 2010 m. vasario 26 d. įsakymu Nr. V.I-26 „Dėl LIMIS duomenų saugos nuostatų patvirtinimo“.

4. Elektroninės informacijos savybės: konfidencialumas – kad su informacinėje sistemoje tvarkoma slapta elektronine informacija gali susipažinti tik tam įgalioti asmenys, vientisumas – kad elektroninė informacija nebūtų atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta, prieinamumas – kad elektroninė informacija gali būti tvarkoma reikiamu metu.

5. LIMIS esanti elektroninė informacija skirstoma į dvi kategorijas, t. y. viešąją informaciją ir neviešąją informaciją.

6. LIMIS saugaus elektroninės informacijos tvarkymo taisyklėse naudojamos LIMIS nuostatuose ir LIMIS duomenų saugos nuostatuose apibrėžtos sąvokos ir trumpinimai.

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. LIMIS centro bendrosioms patalpoms naudojamos šios saugos užtikrinimo priemonės:

7.1. patalpos yra rakinamos;

7.2. yra įrengta ir veikia patalpų signalizacija.

8. LIMIS saugos užtikrinimo priemonės patalpoms (toliau – LIMIS centras), kuriose yra LIMIS tarnybinės stoties kompiuterinė bei programinė įranga:

8.1. patalpa atskirta nuo bendro naudojimo patalpų, durys yra rakinamos;

8.2. asmenys, nesusiję su LIMIS administravimu, patekti į šias patalpas gali tik LIMIS centro darbuotojų lydimi;

8.3. patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės, vykdoma gaisro gesinimo priemonių patikra;

8.4. įrengta ir veikia kondicionavimo sistema, nuolat stebimi temperatūros ir drėgmės svyravimai;

8.5. techninė įranga saugoma nuo elektros srovės svyravimų nepertraukiamo maitinimo šaltiniais (UPS), kurie turi užtikrinti informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne mažiau nei 10 min.;

8.6. įrengta ir veikia patalpų signalizacijos sistema.

9. LIMIS taikomos šios techninės, sisteminės ir taikomosios programinės saugos užtikrinimo priemonės:

9.1. LIMIS naudotojai naudojasi Saugaus valstybinio duomenų perdavimo tinklo (SVDPT) paslaugomis, o nutolusių padalinių bei nutolusių kompiuterizuotų darbo vietų (KDV) apsaugai ir prijungimui naudojama „Netscreen“ įranga bei VPN;

9.2. išorinis prisijungimas prie vidinio duomenų perdavimo tinklo yra kontroliuojamas;

9.3. informacinėje sistemoje turi būti registruojami ir nustatytą laiką saugomi duomenys apie sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, kitus saugai svarbius įvykius, nurodant LIMIS naudotojo identifikatorių ir įvykio laiką;

9.4. tinklu siunčiama konfidenciali informacija yra šifruojama;

9.5. tinklo maršrutai yra griežtai nustatyti ir duomenų perdavimo tinklo būklė yra stebima;

9.6. LIMIS naudotojų teisė naudotis programine įranga yra valdoma;

9.7. naudojama tik sertifikuota ir legali programinė įranga;

9.8. kompiuterizuotose darbo vietose įdiegtos tinklinės antivirusinės programos;

9.9. reguliariai daromos duomenų bazių ir kitos svarbios informacijos kopijos;

9.10. atsarginės duomenų ir programinės įrangos kopijos saugomos nedegioje spintoje, esančioje kitoje patalpoje;

9.11. įranga prižiūrima pagal gamintojo rekomendacijas;

9.12. gedimų šalinimą atlieka kvalifikuoti specialistai;

9.13. svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima;

9.14. informacinės sistemos naudotojai apmokomi dirbti su programine įranga;

9.15. tinklo kabeliai apsaugoti nuo neteisėto prisijungimo prie tinklo ir jų pažeidimo;

9.16. LIMIS turi perspėti LIMIS-C administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

10. LIMIS naudotojai, pasirašę konfidencialumo pasižadėjimą, užregistruojami LIMIS-C, jiems suteikiami vartotojų vardai, slaptažodžiai bei prieigos teisės pagal jų pareigybių aprašymuose nustatytas funkcijas.

11. Parengiamas ir atnaujinamas veiklos tęstinumo valdymo planas, reglamentuojantis veiklos tęstinumo užtikrinimą.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

12. Duomenų keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

12.1. LIMIS elektroninių katalogų duomenis LIMIS-M posistemyje įveda, keičia, atnaujina ir naikina LM tvarkytojai;

12.2. LM tvarkytojai eksportuoja duomenis į LIMIS-C posistemio duomenų bazę;

12.3. LM tvarkytojų duomenų teikimas į LIMIS-C posistemio duomenų bazę vykdomas prisijungimui naudojant VPN;

12.4. LIMIS duomenys perduodami automatiniu būdu naudojant TCP/IP protokolą realiame laike („ON-line“ režimu) arba asinchroniniu režimu pagal LIMIS duomenų teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

12.5. LIMIS-M posistemių elektroniniuose žurnaluose registruojamas LM tvarkytojų prisijungimo vardas, slaptažodis, kuris turi būti keičiamas ne rečiau nei kas 6 mėn.;

12.6. LIMIS-C posistemio elektroniniuose žurnaluose registruojami LM tvarkytojų duomenų importavimo iš LIMIS-M metu atliekami veiksmai. Ši informacija turi būti prieinama LIMIS-C administratoriui ir saugos įgaliotiniui, siekiant nustatyti galimus duomenų vientisumo pažeidimus;

12.7. LIMIS-C administratorius eksportuoja duomenis į LIMIS-K posistemio duomenų bazę.

13. Duomenų kopijų darymo tvarka:

13.1. LIMIS-C posistemyje atsarginių duomenų kopijos programinėmis priemonėmis daromos kiekvieną savaitę pasirinktą darbo dieną (po darbo valandų);

13.2. pakartotinės LIMIS atsarginių duomenų kopijos daromos prieš ir po posistemių programinių atnaujinimų ar įvedus didelį kiekį naujos elektroninės informacijos;

13.3. atsarginės duomenų kopijos įrašomos į rezervines duomenų saugyklas ir saugomos kitoje patalpoje nedegioje spintoje;

13.4. atsarginių duomenų kopijų darymas fiksuojamas rezervinių duomenų saugyklų žurnale;

13.5. prarasti ar sunaikinti duomenys yra atkuriami iš rezervinių duomenų kopijų;

13.6. LIMIS-C administratorius yra atsakingas už rezervinių duomenų kopijų darymą, periodiškus duomenų atkūrimo iš kopijų bandymus, duomenų atkūrimo ir rezervinių duomenų kopijų apsaugą;

13.7. duomenų saugos įgaliotinis atsakingas už rezervinių duomenų saugojimo kontrolę.

14. Duomenys iš LIMIS-M eksportuojami į LIMIS-C saugoti, archyvuoti ir teikti į LIMIS-K bei į kitus viešuosius katalogus.

15. Duomenys iš anksčiau muziejuose sukurtų rinkinių informacinių sistemų importuojami į LIMIS-C saugoti, archyvuoti ir teikti į LIMIS-K bei į kitus viešuosius katalogus.

16. LIMIS duomenys kitiems viešiesiems katalogams perduodami vadovaujantis LIMIS saugumo politiką įgyvendinančiais dokumentais bei duomenų perdavimą reglamentuojančiais teisės aktais;

17. LM tvarkytojai eksportuojamus duomenis pagal sutartis su LDM teikia į LIMIS-C, vadovaudamiesi teisės aktų ir LIMIS nuostatuose nustatyta tvarka.

18. Neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

18.1. LIMIS-C administratorius ne rečiau kaip 3 kartus per savaitę privalo peržiūrėti turimus LIMIS programinės įrangos elektroninius žurnalus, juose registruojamus įrašus, siekdamas patikrinti, ar su duomenimis nėra vykdoma neteisėta veikla. Ją aptikęs, nedelsdamas apie tai informuoja saugos įgaliotinį;

18.2. LM tvarkytojai, kilus įtarimui, kad su duomenimis yra vykdoma neteisėta veikla, privalo nedelsdami apie tai informuoti LIMIS-C administratorių. LIMIS-C administratorius nedelsdamas turi imtis visų įmanomų veiksmų, reikalingų užkirsti kelią neteisėtai veiklai su duomenimis;

18.3. duomenų saugos įgaliotinis, ne rečiau kaip kartą per 2 metus, atlieka atitikties vertinimą, kurio metu duomenų saugos požiūriu patikrina ne mažiau kaip dešimtadalį LIMIS kompiuterizuotų darbo vietų, jose instaliuotą programinę įrangą, konfigūraciją bei įvertina duomenų realios saugos atitiktis LIMIS saugos nuostatams ir saugą įgyvendinantiems dokumentams;

18.4. LIMIS-C administratorius privalo naudoti visas turimas ir įmanomas technines, programines ir administracines priemones, skirtas apsaugoti duomenis nuo neteisėto jų naudojimo.

19. Programinės įrangos diegimo ar atnaujinimo bei LIMIS kompiuterinės ir techninės įrangos keitimo ar perkėlimo (toliau – pokyčių) tvarka:

19.1. LIMIS pokyčiai gali būti atliekami tik LIMIS valdytojui raštiškai pritarus;

19.2. turi būti laikomasi oficialių įforminimo, testavimo, įgyvendinimo procedūrų atliekant svarbius pokyčius esamoje sistemoje ar diegiant naujus sistemos komponentus;

19.3. prieš atliekant LIMIS pokyčius, kurių metu gali iškilti grėsmė duomenų konfidencialumui, vientisumui ar pasiekiamumui, LIMIS-C administratorius privalo atliekamus pakeitimus patikrinti (testuoti);

19.4. įgyvendinant LIMIS pokyčius, kurių metu galimi LIMIS veikimo sutrikimai, LIMIS-C administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų LIMIS pokyčių vykdymo pradžios informuoti LIMIS naudotojus ir registruotus LIMIS-K naudotojus apie tokių darbų pradžią ir galimus LIMIS veiklos sutrikimus;

19.5. LIMIS-C administratorius LIMIS naudotojams ir registruotiems LIMIS-K naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi LIMIS pakitimus, kurių atsiradimas susijęs su įvykdytais arba vykdomais LIMIS pokyčiais.

IV. REIKALAVIMAI, KELIAMI LIMIS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

20. Reikalavimai, keliami LIMIS funkcionavimui reikalingoms paslaugų teikėjų ir jų projektavimo, aptarnavimo ir priežiūros teikiamoms paslaugoms, nustatomi šių paslaugų teikimo sutartyse.

21. Paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja LIMIS taikomąją programinę įrangą naudodamas:

21.1. įgyvendintas elektroninės informacijos saugos priemones nuo nesankcionuoto poveikio sisteminei, programinei įrangai ir patalpoms;

21.2. sertifikuotą sisteminę programinę įrangą;

21.3. LIMIS testinės duomenų bazės duomenis (LIMIS taikomajai programinei įrangai

modifikuoti).

22. LIMIS-C administratorius atsako už programinių, techninių ir kitų prieigos prie LIMIS resursų organizavimą, suteikimą ir panaikinimą LIMIS techninės ar programinės priežiūros paslaugos teikėjui.

23. LIMIS-C administratorius suteikia LIMIS priežiūros paslaugos teikėjui tik tokią prieigą prie LIMIS resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje numatytus įsipareigojimus.

24. LIMIS-C administratorius privalo supažindinti LIMIS priežiūros paslaugų teikėją su suteiktos prieigos prie LIMIS saugos reikalavimais ir sąlygomis.

25. Pasibaigus sutarties su LIMIS priežiūros paslaugos teikėju galiojimo terminui ar atsiradus kitoms sutartyje ar LIMIS saugos politiką įgyvendinančiuose dokumentuose įvardytoms sąlygoms, LIMIS-C administratorius privalo nedelsdamas organizuoti suteiktos prieigos panaikinimą.

V. BAIGIAMOSIOS NUOSTATOS

26. Asmenys, pažeidę šių Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

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