PATVIRTINTA
Lietuvos dailės muziejaus direktoriaus
2019 m. spalio 25 d. įsakymu Nr. V.1-137

LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (toliau – LIMIS, informacinė sistema) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti minimalius informacinės sistemos elektroninės informacijos (toliau – elektroninė informacija) tvarkymo, techninius ir kitus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus.
2. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Lietuvos integralios muziejų informacinės sistemos duomenų saugos nuostatuose (toliau – informacinės sistemos duomenų saugos nuostatai) ir kituose teisės aktuose bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose.
3. Informacinėje sistemoje tvarkoma elektroninė informacija ir jos grupių sąrašas pateikiami Lietuvos integralios muziejų informacinės sistemos nuostatų (toliau – informacinės sistemos nuostatai), patvirtintų Lietuvos dailės muziejaus direktoriaus 2010 m. vasario 26 d. įsakymo Nr. V.1-25 „Dėl Lietuvos integralios muziejų informacinės sistemos (LIMIS) nuostatų patvirtinimo“, 23–25 punktuose (aktuali redakcija).
4. Už informacinėje sistemoje esančios elektroninės informacijos, priskirtos svarbios elektroninės informacijos kategorijai, tvarkymą atsakingi informacinės sistemos naudotojai.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Kompiuterinės įrangos saugos priemonės:

5.1. turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios informacinėje sistemoje stebėtų įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

5.2. įvykusi įtartina veikla turi būti užfiksuojama audito įrašuose ir automatiškai kuriamas pranešimas informacinės sistemos administratoriui (toliau – administratorius) arba informacinės sistemos lokalios tarnybinės stoties administratoriui (toliau – LIMIS-M administratorius). Sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį;

5.3. įsilaužimo atakų pėdsakai turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie juos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus valandos, jeigu informacinės sistemos valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio informacinės sistemos veiklai vertinimas (testavimas);

5.4. pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą ir įjungtos užkardos, sukonfigūruotos praleisti tik su informacinės sistemos funkcinėmis galimybėmis ir administravimu susijusį duomenų srautą. Užkardų konfigūracijų dokumentacija turi būti saugoma kartu su informacinės sistemos dokumentacija;

5.5. įsilaužimo aptikimo techninių sprendinių užkardos įvykių žurnalai turi būti reguliariai analizuojami, o saugaus elektroninės informacijos tvarkymo saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos. Įsilaužimo aptikimo techninių sprendinių įgyvendinimo tvarkos aprašas, konfigūracijos dokumentacija ir kibernetinių incidentų aptikimo taisyklės (kartu nurodant datas (įgyvendinimo, atnaujinimo ir pan.), atsakingus asmenis, taikymo periodus ir pan.) turi būti saugomos elektronine forma atskirai nuo informacinės sistemos techninės įrangos;

5.6. pagrindinė informacinės sistemos kompiuterinė įranga turi būti dubliuota, turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį kompiuterinės įrangos veikimą ne trumpiau kaip 30 minučių ir apsaugantį nuo elektros srovės svyravimų;

5.7. informacinės sistemos komponentų stebėjimo priemonės turi perspėti administratorių ar LIMIS-M 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, sutrinka kitų informacinės sistemos komponentų įprastas veikimas;

5.8. svarbiausios kompiuterinės įrangos gedimai turi būti registruojami. Už gedimų registravimą atsakingi administratoriai ir LIMIS-M administratoriai;

5.9. informacinės sistemos kompiuterinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

5.10. informacinės sistemos kompiuterinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – administratoriai, LIMIS-M administratoriai arba tokias paslaugas teikiantys paslaugų teikėjai.

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. turi būti reguliariai atliekami iš vidinio kompiuterių tinklo ir viešųjų tinklų pasiekiamų tarnybinių stočių ir atsitiktinai atrinktų naudotojų kompiuterinės įrangos operacinių sistemų, kitos naudojamos programinės įrangos pažeidžiamumų skenavimai;

6.2. turi būti reguliariai atliekama nesankcionuotų įrenginių paieška informacinės sistemos kompiuterių tinkle;

6.3. naudotojų darbo vietose gali būti naudojamos tik tarnybos (darbo) reikmėms skirtos išorinės duomenų laikmenos (pvz., USB atmintinės, kompaktiniai diskai ir kt.) ir jos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinės sistemos tvarkymu;

6.4. atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje kitose patalpose arba kitame pastate nei yra informacinės sistemos tarnybinės stotys;

6.5. turi būti registruojami visi informacinės sistemos duomenų bazių, taikomųjų programų veikimo ir kiti informacinės sistemos darbo sutrikimai.

7. Elektroninės informacijos perdavimo tinklo saugumo užtikrinimo priemonės:

7.1. kompiuterių tinklas turi būti suskirstytas į skirtingo saugumo lygio segmentus pagal informacinės sistemos komponentų atliekamas funkcijas. Informacinės sistemos duomenų bazės ir informacinės sistemos taikomoji programinė įranga negali būti tame pačiame tinklo segmente. Viešai prieinamos informacinės sistemos funkciškai savarankiškos dalys turi būti atskirame tinklo segmente – demilitarizuotoje zonoje;

7.2. elektroninės informacijos perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį jų veikimą ne trumpiau kaip 30 minučių;

7.3. elektroninės informacijos perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

7.4. elektroninės informacijos perdavimo tinklo kabeliai turi būti apsaugoti nuo nesankcionuotos prieigos ir (ar) pažeidimo;

7.5. kitoms valstybės institucijoms, valstybės registrams ir valstybės informacinėms sistemoms, kitoms informacinėms sistemoms elektroninė informacija turi būti perduodama tik saugiais elektroninių ryšių tinklais. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą, nurodyti informacinės sistemos duomenų saugos nuostatuose;

7.6. priemonės, naudojamos informacinės sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais;

7.7. pagrindinėse informacinės sistemos tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su informacinės sistemos funkcionalumu ir administravimu susijusį duomenų srautą. Ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir šalinamos pastebėtos neatitiktys saugumo reikalavimams.

8. Informacinėje sistemoje naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo ir kontrolės priemonės:

8.1. turi būti įgyvendinti atpažinties, tapatumo patvirtinimo ir naudojimosi informacinėmis sistemomis saugumo ir kontrolės reikalavimai, nustatyti Lietuvos integralios muziejų informacinės sistemos naudotojų administravimo taisyklėse;

8.2. draudžiama slaptažodžius saugoti programos tekste;

8.3. svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;

8.4. turi būti įgyvendinti svetainės kriptografijos reikalavimai:

8.4.1. svetainės administravimo darbai turi būti atliekami ne trumpesniu kaip 128 bitų raktu;

8.4.2. šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų;

8.4.3. turi būti naudojamas TLS standartas;

8.4.4. svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje;

8.4.5. visi kriptografiniai moduliai turi turėti galimybę saugiai sutrikti.

8.5. tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro rekomenduojamą testavimo priemonę;

8.6. draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai;

8.7. turi būti naudojama svetainės užkarda. Įsilaužimo atakų pėdsakai turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus valandos, jeigu informacinės sistemos valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio ryšių ir informacinės sistemos veiklai vertinimas (testavimas);

8.8. turi būti naudojamos apsaugos priemonės nuo pagrindinių per tinklą vykdomų atakų: SQL intarpų įterpimas, įterptinių instrukcijų (XSS) atakų, internetinės paslaugos sutrikdymo (DoS) atakų, srautinių internetinės paslaugos sutrikdymo (DDoS) atakų ir kitų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto interneto svetainėje www.owasp.org;

8.9. turi būti vykdoma svetainės naudotojo įvedamų duomenų patikra (angl. validation);

8.10. tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;

8.11. svetainės saugumo priemonės turi būti tokios, kad automatiškai būtų uždraudžiama prieiga prie tarnybinės stoties iš IP adresų, iš kurių buvo vykdoma grėsminga veikla (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir pan.);

8.12. turi būti vykdomas informacinės sistemos naudotojų, LIMIS-M administratorių ir administratorių atliekamų veiksmų auditas ir laikomasi kontrolės reikalavimų;

8.13. tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcinėms galimybėms užtikrinti reikalingus HTTP metodus;

8.14. turi būti uždrausta naršyti svetainės aplankuose;

8.15. turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo stebėsenos sistema.

9. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

9.1. turi būti įrengta patalpų apsaugos signalizacija, kurios signalai persiunčiami patalpas saugantiems budėtojams arba saugos tarnybai;

9.2. darbuotojai, palikdami patalpas ar darbo vietas, turi užrakinti duris ir uždaryti langus;

9.3. visi lankytojai turi būti lydimi informacinės sistemos valdytojo ar tvarkytojo darbuotojų, išskyrus atvejus, kai tokių lankytojų prieiga yra iš anksto patvirtinta. Lankytojams turi būti išduodama svečio kortelė;

9.4. naudotojų darbo vietų aplinka turi atitikti Lietuvos higienos normą HN 32:2004 „Darbas su videoterminalais. Saugos ir sveikatos reikalavimai“, patvirtintą Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. vasario 12 d. įsakymu Nr. V-65 „Dėl Lietuvos higienos normos HN 32:2004 „Darbo su videoterminalais. Saugos ir sveikatos

reikalavimai“ patvirtinimo“, ir kitus Lietuvos Respublikos teisės aktuose nustatytus reikalavimus;

9.5. visose patalpose ir jų sektoriuose turi būti ugnies gesintuvai, įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato apsaugos signalizacijos ir saugos tarnybos stebėjimo pulto, reguliariai atliekama gaisro aptikimo ir gesinimo priemonių patikra.

10. Papildomos tarnybinių stočių patalpų apsaugos nuo neteisėto asmenų patekimo į jas ir kitos saugos užtikrinimo priemonės:

10.1. įsilaužimo davikliai turi būti prijungti prie atskiros signalizacijos zonos;

10.2. patalpose turi būti įrengtos vaizdo stebėjimo sistemos;

10.3. patalpose turi būti dubliuota oro kondicionavimo ir drėgmės kontrolės įranga. Temperatūros ir oro drėgnumo normos turi būti užtikrinamos pagal techninės įrangos gamintojų nustatytus reikalavimus. Patalpų oro kondicionavimo ir drėgmės kontrolės įranga turi turėti automatinę įspėjimo funkciją. Apie neužtikrinamas patalpų oro temperatūros ir oro drėgnumo normas turi būti automatiškai informuojami LIMIS-M administratoriai ar administratoriai;

10.4. patalpose turi būti užtikrinamas nepertraukiamas elektros energijos tiekimas, naudojant alternatyvų elektros energijos tiekimo šaltinį, kurio veikimas turi būti patikrinamas ne rečiau kaip kartą per mėnesį imituojant elektros energijos dingimą. Alternatyvaus elektros energijos tiekimo šaltinio tikrinimai turi būti registruojami žurnale;

10.5. fizinė prieiga suteikiama tik informacinės sistemos valdytojo vadovo įsakymu paskirtiems atsakingiems darbuotojams. Kiti darbuotojai arba tretieji asmenys gali patekti į šias patalpas tik lydimi atsakingų darbuotojų. Kiekvienas patekimas į patalpą turi būti fiksuojamas;

10.6. patalpų raktai turi būti saugomi seife. Pagrindiniai tarnybinių stočių patalpų raktai ir atsarginiai raktai turi būti saugomi atskiruose pastatuose;

10.7. patalpų sienos turi būti sumūrytos iš plytų ar blokelių, lubos turi būti iš gelžbetonio. Patalpose neturi būti langų arba naudojami didelio atsparumo langai specialiais rėmais ir grotomis;

10.8. patalpų durys privalo būti šarvuotos, apsaugotos bent dviem skirtingos konstrukcijos spynomis ir visada rakinamos;

10.9. patalpose turi būti automatinė gaisro gesinimo sistema, įrengti dūmų ir karščio davikliai, prijungti prie patalpų apsaugos signalizacijos ir saugos tarnybos stebėjimo pulto;

10.10. kompiuterinio ryšio linijos turi būti apsaugotos nuo elektros išlydžių, perkūnijos ir elektros linijų avarijų naudojant apsauginius įtaisus su įžeminimo tašku.

11. Naudotojų, LIMIS-M administratorių ir administratorių atliekamų veiksmų audito ir kontrolės reikalavimai:

11.1. informacinėje sistemoje turi būti įrašomi duomenys apie informacinės sistemos tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimą, išjungimą, perkrovimą, sėkmingus ir nesėkmingus naudotojų, LIMIS-M administratoriaus ir administratoriaus prisijungimus/ atsijungimus prie informacinės sistemos tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos, naudotojų / LIMIS-M administratorių / administratorių teisių naudotis informacinės sistemos / tinklo ištekliais pakeitimus, apie visus naudotojų vykdomus veiksmus, audito funkcijos įjungimą / išjungimą, audito įrašų trynimą, kūrimą ar keitimą, laiko ir (ar) datos pakeitimus, kitus elektroninės informacijos saugai svarbius įvykius,

11.2. audito įrašuose turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis / pobūdis, naudotojo / LIMIS-M administratoriaus / administratoriaus ir (arba) informacinės infrastruktūros įrenginio, susijusio su įvykiu, duomenys bei įvykio rezultatas. Šie duomenys, techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti, turi būti saugomi, užtikrinant visas prasmingas jų turinio reikšmes, ne trumpiau kaip vienus metus kitoje, nei jie įrašomi, sistemoje ir analizuojami ne rečiau kaip kartą per savaitę, o apie analizės rezultatus informuojamas kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą;

11.3. informacinės sistemos komponentų įvykių žurnalai turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto ar netyčinio pakeitimo ar sunaikinimo. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas;

11.4. turi būti naudojamos tinkamos audito duomenų rinkimo, analizės, išsaugojimo, autentiškumo užtikrinimo ir pateikimo kompetentingoms institucijoms priemonės. Prieiga prie audito duomenų turi būti kontroliuojama ir pasiekiami tik administratoriams, LIMIS-M administratoriams ir kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis);

11.5. audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu;

11.6. dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant, bet ne vėliau kaip vieną darbo dieną turi būti informuojamas administratorius ir kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą;

11.7. turi būti daromos audito įrašų duomenų kopijos, kurios turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

12. Informacinės sistemos vienkartinis neveikimo laikotarpis negali būti ilgesnis nei 12 val., o per metus prieinamumas turi būti užtikrintas ne mažiau kaip 96 proc. viso paros laiko.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

13. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

13.1. elektroninė informacija į informacinę sistemą gali būti įvedama, joje keičiama, atnaujinama ir naikinama tik Taisyklių, informacinės sistemos nuostatų, informacinės sistemos duomenų saugos nuostatų ir kitų teisės aktų, reglamentuojančių informacinės sistemos veiklą ir elektroninės informacijos tvarkymą, nustatyta tvarka;

13.2. elektroninė informacija gali būti tvarkoma pagal naudotojams, LIMIS-M administratoriams ir administratoriams suteiktas prieigos teises ir tik turint teisėtą tikslą ir pagrindą;

13.3. informacinėje sistemoje esančiomis elektroninės informacijos naikinimo priemonėmis turi būti užtikrinta, kad nebūtų galima atkurti sunaikintos elektroninės informacijos;

13.4. turi būti užtikrinama asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolė ir ištrynimas po jų panaudojimo perkeliant į duomenų bazes ir pan.

13.5. turi būti fiksuojami šie naudotojų, kuriems suteikta teisė tvarkyti duomenis, prisijungimų prie duomenų bazės įrašai: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas), bylos, prie kurių buvo jungtasi, ir su duomenimis

atlikti veiksmai (įvedimas, peržiūra, keitimas, naikinimas ar kiti duomenų tvarkymo veiksmai). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus;

13.6. naudotojui prisijungus prie informacinės sistemos, bet neatliekant jokių veiksmų 15 minučių, informacinės sistemos taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartotinai atlikus savo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

13.7. naudotojui baigus darbą ar pasitraukus iš darbo vietos, turi būti automatiškai užtikrinama, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu; dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;

13.8. naudotojų kompiuteriuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungta lygiarangių (angl. *peer to peer*) naudojimo funkcinė galimybė, belaidė periferinė prieiga;

13.9. informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo, patikimumo tikrinimo ir informavimo apie klaidas priemones.

14. Atsarginių elektroninės informacijos kopijų darymas, saugojimas, elektroninės informacijos atkūrimo iš atsarginių kopijų išbandymas vykdomas vadovaujantis informacinės sistemos duomenų saugos nuostatuose nustatyta tvarka.

15. Elektroninė informacija perkeliama ir teikiama į susijusius registrus ar kitas informacines sistemas ir iš jų gaunama vadovaujantis Taisyklių 3 punkte nurodytuose teisės aktuose nustatyta tvarka ir sąlygomis.

16. Neteisėtos veiklos – elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo – nustatymo tvarka:

16.1. siekiant nustatyti, ar su informacinėje sistemoje esančia elektronine informacija nėra vykdoma neteisėta veikla, visi elektroniniuose įvykių žurnaluose saugomi įrašai turi būti analizuojami ne rečiau kaip kartą per savaitę;

16.2. naudotojai, pastebėję informacinės sistemos kibernetinio saugumo ir (ar) elektroninės informacijos saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos ar kibernetinio saugumo užtikrinimo priemones, įvykius ar veiką, atitinkančią kibernetinio ar elektroninės informacijos saugos incidento požymius, arba apie tai gavę informacijos iš kitų informacijos šaltinių, privalo nedelsdami apie tai pranešti informacinės sistemos saugos įgaliotiniui arba informacinės sistemos kibernetinio saugumo vadovui;

16.3. informacinės sistemos saugos įgaliotinis arba informacinės sistemos kibernetinio saugumo vadovas, įtaręs, kad su elektronine informacija yra vykdoma neteisėta veikla, inicijuoja elektroninės informacijos saugos ar kibernetinių incidentų valdymo procedūras.

17. Informacinės sistemos programinės ir techninės įrangos keitimo, informacinės sistemos pokyčių valdymo tvarka nustatyta Taisyklių priede „Pokyčių valdymo tvarkos aprašas“.

18. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau – mobilieji įrenginiai) naudojimo tvarka:

18.1. mobiliesiems įrenginiams, naudojamiems informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpose, esantiems vidiniame informacinės sistemos kompiuterių tinkle, taikomi tokie patys elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai kaip ir stacionariesiems kompiuteriams;

18.2. leidžiama naudoti tik mobiliuosius įrenginius, atitinkančius informacinės sistemos valdytojo nustatytus saugumo reikalavimus;

18.3. informacinės sistemos valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą;

18.4. iš mobiliųjų įrenginių draudžiama tiesiogiai nuotoliniu būdu prisijungti prie informacinės sistemos informacinių technologijų infrastruktūros. Prisijungimas galimas tik per tarpinį įrenginį, naudojantis virtualiuoju privačiuoju tinklu (VPN), atitinkančiu saugos politikos įgyvendinimo dokumentuose nustatytus organizacinius ir techninius elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

18.5. prie tarpinio įrenginio leidžiamų prisijungti mobiliųjų įrenginių sąrašą tvirtina informacinės sistemos tvarkytojo vadovas;

18.6. naudojant priemones, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius, turi būti reguliariai tikrinami tarpiniai įrenginiai ir mobilieji įrenginiai apie neleidžiamus ar saugumo reikalavimų neatitinkančius tarpinius įrenginius ar mobiliuosius įrenginius turi būti pranešama informacinės sistemos saugos įgaliotiniui arba informacinės sistemos kibernetinio saugumo vadovui;

18.7. turi būti parengti mobiliųjų įrenginių operacinių sistemų atvaizdai su saugumo nuostatomis, kuriuose nustatyti veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos, taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi, atnaujinami ir iškart atnaujinami nustačius naujų pažeidžiamų vietų ar atakų;

18.8. pagal parengtus atvaizdus į mobiliuosius įrenginius turi būti įdiegiama operacinė sistema su saugumo nuostatomis;

18.9. 7mobilieji įrenginiai, kuriais naršoma internete, privalo būti apsaugoti nuo judriųjų programų keliamų grėsmių;

18.10. mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo kontrolės priemonės, automatiškai apribojančios neleidžiamo vykdomojo kodo naudojimą ar informuojančios administratorių apie neleidžiamo vykdomojo kodo naudojimą;

18.11. mobilieji įrenginiai turi būti apsaugoti slaptažodžiu, sudaromu ir tvarkomu Lietuvos integralios muziejų informacinės sistemos naudotojų administravimo taisyklėse nustatyta tvarka. Jeigu mobiliajame įrenginyje naudojama mobiliojo ryšio kortelė, ji turi būti apsaugota PIN kodu, kuris neturi būti sudaromas iš asmeninės informacijos (pvz., gimimo datos ir pan.) ar lengvai atspėjamo skaičių derinio;

18.12. elektroninė informacija ir kita nevieša informacija, laikoma mobiliuosiuose įrenginiuose (tiek mobiliųjų įrenginių laikmenose, tiek ir išorinėse kompiuterinėse laikmenose), turi būti užšifruota;

18.13. mobiliųjų įrenginių kenksmingos programinės įrangos aptikimo, elektroninės informacijos šifravimo ir kita programinė įranga turi būti įsigyjama tik iš patikimų ir oficialių tiekėjų teisės aktų nustatyta tvarka;

18.14. mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungta lygiarangių naudojimo funkcinė galimybė, belaidė periferinė prieiga;

18.15. mobilieji įrenginiai viešose vietose negali būti palikti be priežiūros. Mobilusis įrenginys, kuriuo nesinaudojama 15 min., turi automatiškai užsirakinti;

18.16. mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį;

18.17. prie mobiliųjų įrenginių draudžiama prijungti jiems nepriklausančius įrenginius.

19. Belaidžio tinklo saugumo priemonės:

19.1. leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus;

19.2. turi būti vykdoma belaidžių įrenginių kontrolė:

19.2.1. tikrinami eksploatuojami belaidžiai įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius;

19.2.2. naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą;

19.2.3. leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidės prieigos taškus;

19.3. belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje;

19.4. prisijungiant prie belaidžio tinklo, turi būti taikomas ryšių ir informacinės sistemos naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas;

19.5. turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą;

19.6. turi būti uždrausti visi nebūtini valdymo protokolai;

19.7. turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai;

19.8. turi būti uždraustas lygiarangis funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje;

19.9. belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu;

19.10. prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINEI SISTEMAI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

20. Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjas, darbų atlikėjas ar prekių tiekėjas (toliau – tiekėjas) turi atitikti informacinės sistemos veiklą reglamentuojančių teisės aktų, standartų, Taisyklių reikalavimus tiekėjo kompetencijai, patirčiai, teikiamoms paslaugoms, atliekamiems darbams ar tiekiamoms prekėms ir rekomendacijas dėl jų, iš anksto nustatytus paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose.
21. Perkant paslaugas, darbus ar prekes, susijusius su informacine sistema, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi būti nustatoma, kad tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, nustatytiems reikalavimams. Perkamos paslaugos, darbai ar prekės, susiję su informacine sistema, turi atitikti teisės aktų ir

standartų, kuriais vadovaujamasi užtikrinant elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar prekių tiekimo pirkimo dokumentuose.

22. Tiekėjas, vykdydamas sutartinius įsipareigojimus, turi įgyvendinti tinkamas organizacines ir technines priemones, skirtas informacinei sistemai ir joje tvarkomai elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.
23. Tiekėjui prieiga prie informacinės sistemos gali būti suteikiama tik pasirašius sutartį, kurioje turi būti nustatytos tiekėjo teisės, pareigos, prieigos prie informacinės sistemos lygiai ir sąlygos, elektroninės informacijos saugos, kibernetinio saugumo, konfidencialumo reikalavimai ir atsakomybė už jų nesilaikymą. Administratorius turi supažindinti tiekėją su suteiktos prieigos prie informacinės sistemos saugos ir kibernetinio saugumo reikalavimais ir sąlygomis. Administratorius yra atsakingas už prieigos prie informacinės sistemos tiekėjui suteikimą ar panaikinimą pasirašius sutartį, pasibaigus sutarties su tiekėju galiojimo terminui ar kitais sutartyje nurodytais prieigos prie informacinės sistemos panaikinimo atvejais.
24. Tiekėjui suteikiamas tik toks prieigos prie informacinės sistemos lygis, kuris yra būtinas sutartyje nustatytiems įsipareigojimams vykdyti. Tiekėjo paskirti specialistai, kurie vykdys sutartį, turi pasirašyti konfidencialumo pasižadėjimus.
25. Iškilus poreikiui, siekdamas įsitikinti, ar tinkamai vykdoma sutartis, laikomasi elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų, informacinės sistemos valdytojas turi teisę atlikti tiekėjo teikiamų paslaugų stebėseną ir auditą, suteikti galimybę atlikti auditą trečiosioms šalims.
26. Tiekėjas privalo nedelsdamas informuoti informacinės sistemos valdytoją apie sutarties vykdymo metu pastebėtus elektroninės informacijos saugos ar kibernetinius incidentus, pastebėtas neveikiančias arba netinkamai veikiančias saugos ar kibernetinio saugumo užtikrinimo priemones, elektroninės informacijos saugos ar kibernetinio saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, saugumo spragas, pažeidžiamas vietas, kitus svarbius saugai įvykius.
27. Informacinės sistemos valdytojas su interneto paslaugų teikėju (-ais) turi būti sudaręs sutartis dėl apsaugos nuo informacinės sistemos elektroninių paslaugų trikdžių, reagavimo į kibernetinius incidentus įprastomis darbo valandomis ir po darbo valandų, nepertraukiamo interneto paslaugos teikimo ir interneto paslaugos sutrikimų registravimo 24 valandas per parą, 7 dienas per savaitę.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

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

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie
Krašto apsaugos ministerijos
2019 m. spalio 21 d. raštu Nr. (4.2)6K-678

Lietuvos integralios muziejų informacinės sistemos
Saugaus elektroninės informacijos tvarkymo taisyklių
priedas

LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS POKYČIŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Pokyčių valdymo tvarkos aprašas (toliau – Aprašas) nustato standartizuotą funkcinių, techninių, programinių, organizacinių ir administracinių Lietuvos integralios muziejų informacinės sistemos (toliau – informacinė sistema) pokyčių (toliau – pokyčiai) valdymą ir kontrolę, siekiant sumažinti neigiamo pokyčių poveikio informacinės sistemos darbui riziką, užtikrinant saugų ir kokybišką reikalingų pokyčių įvykdymą.
2. Apraše nustatyti standartizuoti pokyčių valdymo planavimo procesai, apimantys pokyčių identifikavimą, inicijavimą ir suskirstymą į kategorijas pagal pokyčio tipą, įtakos vertinimą, pokyčių prioritetų nustatymą, pokyčių atlikimą, dokumentavimą, pokyčių valdymo efektyvumo vertinimą.
3. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Lietuvos integralios muziejų informacinės sistemos duomenų saugos nuostatuose (toliau – informacinės sistemos duomenų saugos nuostatai) ir kituose teisės aktuose bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose.

II SKYRIUS
POKYČIŲ IDENTIFIKAVIMAS

4. Pokyčiai identifikuojami analizuojant vidinę ir išorinę informacinės sistemos valdytojo ir tvarkytojų veiklos aplinką ir poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai,

technologiniai aspektai ir tendencijos, esama padėtis (informacinės sistemos sąranka, pažeidžiamumas, atitiktis teisės aktų ir standartų reikalavimams ir pan.).

5. Vidinė ir išorinė informacinės sistemos valdytojo ir tvarkytojų veiklos aplinkos analizė atliekama informacinės sistemos rizikos vertinimo, grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinės sistemos kibernetiniam saugumui, rizikos vertinimo, informacinių technologijų saugos atitikties vertinimo, informacinės sistemos būklės, veiklos efektyvumo ir pajėgumo, elektroninių paslaugų kokybės, atitikties teisės aktų ir standartų reikalavimams ir kitų vertinimų, atliekamų Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo, informacinės sistemos duomenų saugos nuostatų, Lietuvos integralios muziejų informacinės sistemos nuostatų ir kitų informacinės sistemos valdytojo, informacinės sistemos tvarkytojų veiklą reglamentuojančių teisės aktų nustatyta tvarka, metu.
6. Planuojami pokyčiai turi atitikti Lietuvos Respublikos Vyriausybės ar Lietuvos Respublikos Seimo patvirtintus planavimo dokumentus, Lietuvos Respublikos Vyriausybės nustatytas taikomų informacinių ir ryšių technologijų tobulinimo ir plėtros kryptis ir rekomenduojamus taikyti techninius reikalavimus (standartus), informacinės sistemos valdytojo strateginius veiklos planus ir kitus planavimo dokumentus.

III SKYRIUS
POKYČIŲ INICIJAVIMAS IR SKIRSTYMAS Į KATEGORIJAS

7. Pokyčius inicijuoti turi teisę informacinės sistemos valdytojas, informacinės sistemos tvarkytojai, duomenų valdymo įgaliotinis, informacinės sistemos saugos įgaliotinis, informacinės sistemos kibernetinio saugumo vadovas ir informacinės sistemos administratorius (toliau – administratorius) arba informacinės sistemos lokalios tarnybinės stoties administratorius (toliau – LIMIS-M administratorius). Funkciniai, techniniai ir programiniai informacinės sistemos pokyčiai, išskyrus organizacinius ir administracinius pokyčius, turi būti aprašomi rašytine forma ir registruojami. Organizaciniai ir administraciniai pokyčiai aprašomi laisva forma ir saugomi už dokumentų valdymą atsakinguose informacinės sistemos valdytojo struktūriniuose padaliniuose.
8. Registruojami pokyčiai, atsižvelgiant į jų svarbą, aktualumą ir poreikį, skirstomi į šias kategorijas:
   8.1. standartiniai pokyčiai, kurie nekelia rizikos kokybiškam elektroninių paslaugų teikimui arba visos informacinių technologijų infrastruktūros veikimui (pvz., naujos kompiuterinės darbo vietos parengimas informacinės sistemos naudotojui ar informacinės sistemos komponentų pakeitimas, standartinės programinės įrangos įdiegimas, atnaujinimas ar išdiegimas, saugumo spragų pataisų įdiegimas informacinės sistemos naudotojo kompiuterinėje darbo vietoje ir pan.). Standartiniai pokyčiai atliekami Apraše ir kituose informacinės sistemos valdytojo ir informacinės sistemos tvarkytojų priimtuose teisės aktuose nustatyta tvarka;
   8.2. skubūs pokyčiai, kurie skirti aukščiausio prioriteto sutrikimams arba problemoms šalinti ir reikalauja ypatingos įvertinimo, patvirtinimo ir atlikimo skubos, taip pat avariniai pokyčiai (pvz., veiklos atkūrimas likviduojant informacinės sistemos elektroninės informacijos (toliau – elektroninė informacija) saugos ar kibernetinio incidento, stichinės nelaimės, avarijos ar kitų ekstremalių situacijų padarinius). Įvykus avariniams pokyčiams gali būti praleisti pokyčių įtakos vertinimo ir dokumentavimo etapai, tačiau jie turi būti atlikti pašalinus aukščiausio prioriteto sutrikimus arba problemas;

8.3. plėtros (vystymo) pokyčiai, kai kuriamos arba modernizuojamos informacinių technologijų paslaugos ir su tuo susiję veiksmai nėra visiškai aiškūs, o pokyčių atlikimas yra susijęs su tam tikra rizika elektroninių paslaugų teikimui arba visos informacinių technologijų infrastruktūros veikimui.

9. Prioritetas turi būti skiriamas skubiems ir plėtros (vystymo) pokyčiams. Pokyčių prioritetas nustatomas pokyčių įtakos vertinimo metu.

IV SKYRIUS
POKYČIŲ ĮTAKOS VERTINIMAS

10. Informacinės sistemos funkcinių, programinių ir techninių pokyčių įtaką pagal kompetenciją vertina Lietuvos dailės muziejaus filialas Lietuvos muziejų informacijos, skaitmeninimo ir LIMIS centras (toliau – LM ISC LIMIS). Sudėtingų pokyčių įtakai įvertinti iš informacinės sistemos valdytojo kompetentingų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis (toliau – darbuotojai), prireikus – iš nepriklausomų ekspertų gali būti sudaroma darbo grupė.
11. Pokyčių įtakos vertinimo metu turi būti įvertinama pokyčių nauda, pagrįstumas, įgyvendinamumas ir alternatyvūs sprendimai, pokyčiams atlikti reikalingos sąnaudos, taip pat informacinės sistemos darbo sutrikdymo ar sustabdymo rizika, elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo pažeidimo rizika.
12. Jeigu pokyčių įtakos vertinimo metu nustatoma, kad informacinei sistemai kurti ar modernizuoti planuojama viršyti Lietuvos Respublikos Vyriausybės ar jos įgaliotos institucijos patvirtintą lėšų dydį, turi būti rengiama galimybių studija.

V SKYRIUS
POKYČIŲ ATLIKIMAS

13. Funkcinius, techninius, programinius informacinės sistemos pokyčius vykdo LIMIS-M administratoriai, administratoriai arba Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka atrinktas paslaugų teikėjas. Organizacinius ir administracinius pokyčius vykdo už informacinės sistemos palaikymą ir priežiūrą atsakingi informacinės sistemos valdytojo struktūriniai padaliniai.
14. Visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su informacinės sistemos duomenų valdymo įgaliotiniu ir vykdomi tik gavus jo ir informacinės sistemos valdytojo direktoriaus rašytinį pritarimą.
15. Pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri yra atskirta nuo eksploatuojamos informacinės sistemos. Eksploatuojamos informacinės sistemos aplinkoje pokyčiai gali būti vykdomi tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių (pvz., veiklos atkūrimo ar kitos avarinės situacijos) nėra galimybės jų patikrinti bandomojoje informacinės sistemos aplinkoje.
16. Nustačius, kad informacinės sistemos pokyčių bandomojoje aplinkoje rezultatas atitinka laukiamus rezultatus, pokyčiai gali būti atliekami eksploatuojamos informacinės sistemos aplinkoje.

17. Nustatytu darbo laiku gali būti vykdomi tik skubūs ir standartiniai pokyčiai. Plėtros (vystymo) pokyčiai turi būti atliekami po darbo valandų arba savaitgaliais.
18. LIMIS-M administratoriai ar administratoriai turi informuoti informacinės sistemos naudotojus, susijusių registrų ir kitų informacinių sistemų tvarkytojus, kitus suinteresuotus asmenis apie pokyčius, kuriuos įgyvendinant galimi informacinės sistemos darbo sutrikimai. Apie pokyčius informuojama informacinės sistemos viešojoje interneto svetainėje, informacinės sistemos taikomosiose programose ar kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir pan.) ne vėliau kaip likus vienai darbo dienai iki planuojamo pokyčio įgyvendinimo pradžios. Šis punktas netaikomas, jeigu įgyvendinami skubūs pokyčiai.

VI SKYRIUS
POKYČIŲ DOKUMENTAVIMAS

19. Informacinės sistemos sąrankos aprašai turi rodyti esamą informacinės sistemos sąrankos būklę. Informacinės sistemos sąranka ir būsenos rodikliai turi būti tikrinami (peržiūrimi) reguliariai, ne rečiau kaip kartą per metus. Visi įgyvendinti pokyčiai, išskyrus avarinius, turi būti registruojami tam skirtame žurnale.
20. Įgyvendinus pokytį eksploatuojamos informacinės sistemos aplinkoje, LIMIS-M administratoriai ar administratoriai turi patikrinti (peržiūrėti) informacinės sistemos sąranką ir būsenos rodiklius, palyginti ir pagal kompetenciją įvertinti, ar pokytis atitinka planuojamus rezultatus. Sudėtingų ir specifinių pokyčių rezultatams įvertinti gali būti pasitelkti ir kiti informacinės sistemos valdytojo darbuotojai ar trečiosios šalies kompetentingi specialistai.
21. Pokyčiai, susiję su informacinės sistemos kūrimu ar modernizavimu, turi būti dokumentuojami informacinės sistemos techniniuose aprašuose (specifikacijose), tvirtinami ir derinami Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, nustatyta tvarka.

VII SKYRIUS
POKYČIŲ VALDYMO EFEKTYVUMO VERTINIMAS

22. Siekiant efektyvaus pokyčių valdymo, turi būti analizuojami ir vertinami šie rodikliai:
    22.1. informacinės sistemos veiklos sutrikimų ar elektroninės informacijos klaidų, kilusių dėl netikslios specifikacijos ar nepakankamo pokyčių įtakos vertinimo, skaičius;
    22.2. informacinės sistemos taikomųjų programų ar informacinių technologijų infrastruktūros taisymų dėl netinkamos pokyčių specifikacijos skaičius;
    22.3. pokyčių, kurie vyksta pagal Aprašą, procentas.
23. Pokyčių valdymo efektyvumo vertinimą atlieka LM ISC LIMIS.

VIII SKYRIUS
POKYČIŲ VALDYMO PROCESAS

24. Pokyčių valdymo procesas vykdomas atsižvelgiant į Aprašo, Informacinių technologijų paslaugų valdymo metodikos, patvirtintos Informacinės visuomenės plėtros komiteto prie

Susisiekimo ministerijos direktoriaus 2013 m. birželio 19 d. įsakymu Nr. T-83 „Dėl Informacinių technologijų paslaugų valdymo metodikos patvirtinimo“ reikalavimus.

_____