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

LIETUVOS INTEGRALIOS MUZIEJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos integralios muziejų informacinės sistemos (toliau – LIMIS, informacinė sistema) duomenų saugos nuostatuose (toliau – Saugos nuostatai) nustatomi principai ir taisyklės, užtikrinantys saugų informacinės sistemos elektroninės informacijos tvarkymą (gavimą, įvedimą, apdorojimą, saugojimą, teikimą) informacinių technologijų ir ryšio priemonėmis.
2. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), vartojamas sąvokas.
3. Saugos nuostatai reguliuoja saugų informacinės sistemos elektroninės informacijos tvarkymą ir yra privalomi visiems informacinės sistemos elektroninę informaciją tvarkantiems fiziniams ir juridiniams asmenims, administratoriams, kibernetinio saugumo vadovui ir saugos įgaliotiniui.
4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:
   4.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;
   4.2. informacinės sistemos veiklos tęstinumo užtikrinimas;
   4.3. asmens duomenų apsauga;
   4.4. naudotojų mokymas;
   4.5. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė.
5. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:
   5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos elektroninę informaciją;
   5.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;
   5.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų prevenciją, reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus ir juos operatyviai suvaldyti, atkuriant įprastinę informacinės sistemos veiklą.
6. Informacinės sistemos valdytojas yra Lietuvos dailės muziejus, kurio adresas – Didžioji g. 4, LT-01128 Vilnius.
7. Informacinės sistemos pagrindinis tvarkytojas yra Lietuvos dailės muziejus, kurio adresas – Didžioji g. 4, LT-01128 Vilnius.

8. Informacinės sistemos tvarkytojai yra fiziniai ir juridiniai asmenys, sudarę sutartis su Lietuvos dailės muziejumi dėl darbo su informacine sistema, kaupiantys savo elektroninių katalogų duomenis informacinės sistemos duomenų bazėse, viešinantys sklaidai skirtus duomenis informacinės sistemos viešosiose prieigose ir teikiantys informacinėje sistemoje saugomą skaitmeninį turinį į kitas duomenų bazes. Informacinės sistemos tvarkytojų sąrašas yra tvirtinamas Lietuvos dailės muziejaus direktoriaus įsakymu. Šis sąrašas nėra baigtinis. Jis Lietuvos dailės muziejaus direktoriaus įsakymu gali būti papildytas ir kitais fiziniais ir juridiniais asmenimis, gavus prašymą suteikti jiems informacinės sistemos tvarkytojų teises. Lietuvos dailės muziejaus direktoriaus 2019 m. rugpjūčio 14 d. įsakymu Nr. V.1-111 „Dėl Lietuvos integralios muziejų informacinės sistemos (LIMIS) tvarkytojų sąrašo patvirtinimo“ informacinės sistemos tvarkytojų teisės yra suteiktos šiems juridiniams asmenims:
   8.1. Akmenės krašto muziejus, kurio adresas K. Kasakausko g. 17, LT-85367 Akmenė;
   8.2. Akmenės rajono Papilės Simono Daukanto gimnazija, kurios adresas Nepriklausomybės g. 62, LT-85245 Papilė, Akmenės r.;
   8.3. Aleksandro Stulginskio universiteto muziejus, kurio adresas Studentų g. 11, LT-53361 Akademija, Kauno r.;
   8.4. Alytaus kraštotyros muziejus, kurio adresas Savanorių g. 6, LT-62142 Alytus;
   8.5. Anykščių Jono Biliūno gimnazija, kurios adresas Liaudiškių g. 49, LT-29126 Anykščiai;
   8.6. Anykščių menų centras, kurio adresas Vilniaus g. 36, LT-29145 Anykščiai;
   8.7. Antano Baranausko ir Antano Vienuolio-Žukausko memorialinis muziejus, kurio adresas A. Vienuolio g. 4, LT-29147 Anykščiai;
   8.8. Antano Mončio namai-muziejus, kurio adresas S. Daukanto g. 16, LT-00135 Palanga;
   8.9. Aštuonračio muziejukas, kurio adresas Vyšnių g. 22, LT-60382 Nemakščiai, Raseinių r.;
   8.10. Aukštaitijos nacionalinio parko ir Labanoro regioninio parko direkcija, kurios adresas Lūšių g. 16, LT-30202 Palūšės k., Ignalinos r.;
   8.11. B. Grincevičiūtės memorialinis butas-muziejus „Beatričės namai“, kurio adresas Vienuolio g. 12-1, LT-01104 Vilnius;
   8.12. Bažnytinio paveldo muziejus, kurio adresas Šv. Mykolo g. 9, LT-01124 Vilnius;
   8.13. Birštono muziejus, kurio adresas Vytauto g. 9, LT-59211 Birštonas;
   8.14. Biržų krašto muziejus „Sėla“, kurio adresas J. Radvilos g. 3, LT-41175 Biržai;
   8.15. Daugyvenės kultūros istorijos muziejus-draustinis, kurio adresas LT- 82206 Burbiškio k., Radviliškio r.;
   8.16. Druskininkų miesto muziejus, kurio adresas M. K. Čiurlionio g. 59, LT-66164 Druskininkai;
   8.17. Elektrėnų savivaldybės literatūros ir meno muziejus, kurio adresas Rungos g. 24, LT-26110 Elektrėnai;
   8.18. Energetikos ir technikos muziejus, kurio adresas Rinktinės g. 2, LT-09312 Vilnius;
   8.19. Europos centro muziejus Europos parkas, kurio adresas LT-15148 Joneikiškių k., Vilniaus r.;
   8.20. Gargždų krašto muziejus, kurio adresas Sodo g. 5, LT-96136 Gargždai, Klaipėdos r.;
   8.21. Geležinkelių muziejus, kurio adresas Geležinkelio g. 16, LT-01047 Vilnius;
   8.22. Generolo Jono Žemaičio Lietuvos karo akademijos muziejus, kurio adresas Šilo g. 5a, LT-10322 Vilnius;
   8.23. Okupacijų ir laisvės kovų muziejus, kurio adresas Aukų g. 2a, LT-01113 Vilnius;
   8.24. Geologijos ir geografijos instituto Mineralų muziejus, kurio adresas Ševčenkos g. 13, LT-03223 Vilnius;

8.25. Ignalinos krašto muziejus, kurio adresas Ateities g. 43, LT-30119 Ignalina;
8.26. Janinos Monkutės-Marks muziejus-galerija, kurios adresas J. Basanavičiaus g. 45, LT-57182 Kėdainiai;
8.27. Jonavos krašto muziejus, kurio adresas J. Basanavičiaus g. 3, LT-55171 Jonava;
8.28. Joniškio istorijos ir kultūros muziejus, kurio adresas Žemaičių g. 14, LT-84143 Joniškis;
8.29. Jono Meko vizualiųjų menų centras, kurio adresas Malūnų g. 8, LT-01109 Vilnius;
8.30. Jurbarko krašto muziejus, kurio adresas Vydūno g. 21, LT-74119 Jurbarkas;
8.31. Kaišiadorių muziejus, kurio adresas Gedimino g. 85, LT-56144 Kaišiadorys;
8.32. Kardinolo V. Sladkevičiaus memorialinis butas-muziejus, kurio adresas M. Valančiaus g. 6, LT-44279 Kaunas;
8.33. Kauno IX forto muziejus, kurio adresas Žemaičių pl. 73, LT-47435 Kaunas;
8.34. Kauno miesto muziejus, kurio adresas M. Valančiaus g. 6, LT-44275 Kaunas;
8.35. Kauno rajono muziejus, kurio adresas Pilies takas 1, LT-54127 Raudondvaris, Kauno r.
8.36. Kauno Tado Ivanausko zoologijos muziejus, kurio adresas Laisvės alėja 106, LT-44253 Kaunas;
8.37. Kauno technologijos universiteto muziejus, kurio adresas: K. Donelaičio g. 73, LT-44029 Kaunas;
8.38. Kelmės krašto muziejus, kurio adresas Dvaro g. 5, LT-86111 Kelmė;
8.39. Kėdainių krašto muziejus, kurio adresas Didžioji g. 19, LT-57255 Kėdainiai;
8.40. Kražių M. K. Sarbievijaus kultūros centras, kurio adresas Kolegijos g. 5, LT-86282 Kražiai, Kelmės r.
8.41. Kintų Vydūno kultūros centro Vydūno muziejus, kurio adresas LT-99050 Kintai, Šilutės r.;
8.42. Kretingos muziejus, kurio adresas Vilniaus g. 20, LT-97104 Kretinga;
8.43. Kultūros paveldo departamentas prie Kultūros ministerijos, kurio adresas Šnipiškių g. 3, LT-09309 Vilnius;
8.44. Kupiškio etnografijos muziejus, kurio adresas Gedimino g. 2, LT-40114 Kupiškis;
8.45. Lazdijų krašto muziejus, kurio adresas Seinų g. 29, LT-67113 Lazdijai;
8.46. Lietuvių kalbos institutas, kurio adresas P. Vileišio g. 5, LT-10308 Vilnius;
8.47. Lietuvos aklųjų istorijos muziejus, kurio adresas Skroblų g. 10, LT-03142 Vilnius;
8.48. Lietuvos banko Pinigų muziejus, kurio adresas Totorių g. 2/8, LT-01121 Vilnius;
8.49. Lietuvos dailės muziejus, kurio adresas Didžioji g. 4, LT-01126 Vilnius;
8.50. Lietuvos etnokosmologijos muziejus, kurio adresas LT-33354 Kulionių k., Molėtų r.;
8.51. Lietuvos geologijos tarnybos Žemės gelmių informacijos centras, kurio adresas Taikos g. 2, LT-2137 Vievis, Elektrėnų sav.;
8.52. Lietuvos gyventojų genocido ir rezistencijos tyrimo centras, kurio adresas Didžioji g. 17/1, LT-01128 Vilnius;
8.53. Lietuvos jūrų muziejus, kurio adresas Smiltynės pl. 3, LT-93100 Klaipėda;
8.54. Lietuvos liaudies buities muziejus, kurio adresas J. Aisčio g. 2, LT-56335, Rumšiškės, Kaišiadorių r.;
8.55. Lietuvos medicinos ir farmacijos istorijos muziejus, kurio adresas Rotušės a. 28, LT-44279 Kaunas;
8.56. Lietuvos nacionalinė M. Mažvydo biblioteka, kurios adresas Gedimino pr. 51, LT- 01504 Vilnius;
8.57. Lietuvos nacionalinis muziejus, kurio adresas Arsenalo g. 1, LT-01143 Vilnius;
8.58. Lietuvos radijo ir televizijos muziejus, kurio adresas S. Konarskio g. 49, LT-03123 Vilnius;

8.59. Lietuvos sporto muziejus, kurio adresas Muziejaus g. 7, LT-44279, Kaunas;
8.60. Lietuvos šaulių sąjungos muziejus, kurio adresas Laisvės al. 34, LT-44240 Kaunas;
8.61. Lietuvos švietimo istorijos muziejus, kurio adresas Vytauto pr. 52, LT-44237 Kaunas;
8.62. Lietuvos teatro, muzikos ir kino muziejus, kurio adresas Vilniaus g. 41, LT-01119 Vilnius;
8.63. Literatūrinis Aleksandro Puškino muziejus, kurio adresas Subačiaus g. 124, LT-11345 Vilnius;
8.64. Lithuanians in Scotland Association (Škotijos lietuvių asociacija), kurios adresas 76 Main Str., G40 1HD Glazgas Jungtinė Karalystė
8.65. Maironio lietuvių literatūros muziejus, kurio adresas Rotušės a. 13, LT-44279 Kaunas;
8.66. Marijampolės kraštotyros muziejus, kurio adresas Vytauto g. 29, LT-68300 Marijampolė;
8.67. Marijos ir Jurgio Šlapelių namas-muziejus, kurio adresas Pilies g. 40, LT-01123 Vilnius;
8.68. Mažeikių Gabijos gimnazijos muziejus, kurio adresas Gabijos takas 1, LT-89112 Mažeikiai;
8.69. Mažeikių muziejus, kurio adresas Burbos g. 9, LT-89218 Mažeikiai;
8.70. Mažosios Lietuvos istorijos muziejus, kurio adresas Didžioji Vandens g. 6, LT-91246 Klaipėda;
8.71. Merkinės krašto muziejus, kurio adresas Dariaus ir Girėno a. 1, LT-65336 Merkinė, Varėnos r.;
8.72. Molėtų krašto muziejus, kurio adresas Inturkės g. 4, LT-33141, Molėtai;
8.73. Muitinės muziejus, kurio adresas Jeruzalės g. 25, LT-08420 Vilnius;
8.74. Nacionalinis M. K. Čiurlionio dailės muziejus, kurio adresas V. Putvinskio g. 55, LT-44248 Kaunas;
8.75. Nacionalinis muziejus Lietuvos Didžiosios Kunigaikštystės valdovų rūmai, kurio adresas Katedros a. 4, LT-01143 Vilnius;
8.76. Nalšios muziejus, kurio adresas Laisvės a. 1, LT-18111 Švenčionys;
8.77. Neringos muziejai, kurio adresas Pamario g. 53, LT-93124 Naglių g. 4, 93123Nida;
8.78. Pagėgių savivaldybės Martyno Jankaus muziejus, kurio adresas LT-99265 Bitėnai, Pagėgių sav.;
8.79. Pakruojo dvaro rūmai, kurių adresas Parko g. 5, LT-83139 Pakruojo k., Pakruojo r.
8.80. Palangos kurorto muziejus, kurio adresas Birutės g. 34 a, LT-00135 Palanga;
8.81. Panevėžio kraštotyros muziejus, kurio adresas Vasario 16-osios g. 23, LT-35185 Panevėžys;
8.82. Pasvalio krašto muziejus, kurio adresas P. Avižonio g. 6, LT-39149 Pasvalys;
8.83. Povilo Stulgos lietuvių tautinės muzikos instrumentų muziejus, kurio adresas L. Zamenhofo g. 12, LT-44287 Kaunas;
8.84. Prienų krašto muziejus, kurio adresas F. Martišiaus g. 13, LT-59118 Prienai;
8.85. Raseinių krašto istorijos muziejus, kurio adresas Muziejaus g. 3, LT-60123 Raseiniai;
8.86. Rašytojo Vinco Krėvės-Mickevičiaus memorialinis muziejus-namas, kurio adresas LT-65332 Subartonių k., Merkinės sen., Varėnos r.;
8.87. Respublikinis Vaclovo Into akmenų muziejus, kurio adresas Salantų g. 2, LT-98271 Mosėdis, Skuodo r.;
8.88. Rietavo Oginskių kultūros istorijos muziejus, kurio adresas L. Ivinskio g. 4, LT-90311 Rietavas;
8.89. Ryšių istorijos muziejus, kurio adresas Rotušės a. 19, LT-44279 Kaunas;
8.90. Rokiškio krašto muziejus, kurio adresas Tyzenhauzų al. 5, LT-42115 Rokiškis;
8.91. Skuodo muziejus, kurio adresas Šaulių g. 3, LT- 98109 Skuodas;

8.92. Sovietinių skulptūrų Grūto parkas, kurio adresas, LT-66441 Grūto k., Druskininkų r.;
8.93. Šiaulių „Aušros“ muziejus, kurio adresas Vytauto g. 89, LT-77155 Šiauliai;
8.94. Šiaulių rajono literatūros muziejus, kurio adresas Naisiai, LT-81473 Šiaulių r.;
8.95. Šilalės Vlado Statkevičiaus muziejus, kurio adresas S. Gaudėšiaus g. 4, LT- 75135 Šilalė;
8.96. Šilutės Hugo Šojaus muziejus, kurio adresas Lietuvininkų g. 36, LT-99179 Šilutė;
8.97. Tauragės krašto muziejus, kurio adresas S. Dariaus ir S. Girėno g. 5, LT-72215 Tauragė;
8.98. Trakų istorijos muziejus, kurio adresas Kęstučio g. 4, LT-21104 Trakai;
8.99. Ukmergės kraštotyros muziejus, kurio adresas Kęstučio a. 5, LT-20114 Ukmergė;
8.100. Utenos kraštotyros muziejus, kurio adresas Utenio a. 3, LT-28248 Utena;
8.101. Valstybės įmonė Valstybinių miškų urėdija Anykščių regioninis padalinys, kurio adresas Vilniaus g. 101, LT-29142 Anykščiai;
8.102. Valstybės įmonė „Automagistralė“, kurios adresas Kauno g. 14, LT-21372 Vievis;
8.103. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Pasieniečių mokykla, kurios adresas Pasieniečių g. 11, Medininkų k., Vilniaus r.;
8.104. Valstybinio Kernavės kultūrinio rezervato direkcijos Kernavės archeologinės vietovės muziejus, kurio adresas Kerniaus 4 a., Kernavė, LT-19172 Širvintų r.;
8.105. Valstybinis Vilniaus Gaono žydų muziejus, kurio adresas Naugarduko g. 10/2, LT-01141 Vilnius;
8.106. Venclovų namai-muziejus, kurio adresas kurios adresas Pamėnkalnio g. 34, LT-01114 Vilnius;
8.107. Vilkaviškio krašto muziejus, kurio adresas LT-70372 Paežerių k., Vilkaviškio r.;
8.108. Vilniaus dailės akademijos muziejus, kurio adresas Maironio g. 6, LT-01124 Vilnius;
8.109. Vilniaus krašto etnografijos muziejus, kurio adresas Švenčionių g. 14, LT-15168 Nemenčinė, Vilniaus r.;
8.110. Vilniaus memorialinių muziejų direkcija, kurios adresas Pamėnkalnio g. 34, LT-01114 Vilnius;
8.111. Vilniaus universiteto muziejus, kurio adresas Šv. Jono g. 12, LT-01123 Vilnius;
8.112. Vilniaus universiteto medicinos fakulteto Medicinos istorijos muziejus, kurio adresas M. K. Čiurlionio g. 21, LT-03101 Vilnius;
8.113. Vinco Krėvės-Mickevičiaus memorialinis muziejus, kurio adresas Tauro g. 10-1, LT-01114 Vilnius;
8.114. Vinco Mykolaičio Putino memorialinis butas-muziejus, kurio adresas Tauro g. 10-3, LT-01114 Vilnius;
8.115. Visagino „Gerosios vilties“ progimnazija, kurios adresas Partizanų g. 2/7, LT-31105 Visaginas;
8.116. Vytauto Didžiojo karo muziejus, kurio adresas K. Donelaičio g. 64, LT-44248 Kaunas;
8.117. Vyskupo Motiejaus Valančiaus gimtinės muziejus, kurio adresas LT-97330 Nasrėnų k., Kretingos r.;
8.118. Vladislovo Sirakomlės muziejus, kurio adresas Sirokomlės g. 5, LT-13176 Bareikiškių k., Vilniaus r.;
8.119. Viešoji įstaiga „Akmenės istorijos muziejus“, kurios adresas Sodo g. 7-2, LT-85361 Akmenė;
8.120. Zanavykų krašto muziejus, kurio adresas Muziejaus g. 1, LT-71131 Girėnų k., Šakių r.;
8.121. Zarasų krašto muziejus, kurio adresas D. Bukonto g. 20/1, LT-32132 Zarasai;
8.122. Žaislų muziejus, kurio adresas Barboros Radvilaitės g. 7 / Šiltadaržio g. 2, LT-01124 Vilnius;

8.123.Žemaičių dailės muziejus, kurio adresas Parko g.1, LT-90117 Plungė.

8.124.Žemaičių muziejus „Alka“, kurio adresas Muziejaus g. 31, LT-87357 Telšiai.

9. Informacinės sistemos valdytojo funkcijos:

9.1. skiria informacinės sistemos saugos įgaliotinį (toliau – saugos įgaliotinis) ir kibernetinio saugumo vadovą;

9.2. organizuoja informacinės sistemos elektroninės informacijos saugos teisinės bazės plėtojimą ir įgyvendinimą;

9.3. ne rečiau kaip kartą per metus organizuoja saugos dokumentų peržiūrą;

9.4. tvirtina saugos nuostatus, informacinės sistemos saugos politiką įgyvendinančius teisės aktus, kitus dokumentus, tikrina, kaip jie vykdomi;

9.5. užtikrina veiksmingą ir spartų informacinės sistemos tobulinimo planavimą;

9.6. kontroliuoja, kad būtų skiriami pakankami, racionaliai ir taupiai naudojami darbo, materialiniai ir finansiniai ištekliai, susiję su informacinės sistemos tvarkymu;

9.7. atsako už informacinės sistemos tvarkomos informacijos tvarkymo teisėtumą ir elektroninės informacijos saugą.

9.8. atlieka elektroninės informacijos tvarkymo ir elektroninės informacijos saugos bei kibernetinio saugumo reikalavimų laikymosi priežiūrą;

9.9. nagrinėja informacinės sistemos tvarkytojų pasiūlymus dėl informacinės sistemos veiklos, elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

9.10. priima sprendimus:

9.10.1.dėl informacinės sistemos veiklos, elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

9.10.2.dėl informacinės sistemos techninių ir programinių priemonių, būtinų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įsigijimo, diegimo ir modernizavimo;

9.10.3.dėl elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo;

9.11. planuoja veiksmingą ir spartų informacinės sistemos pokyčių valdymą;

9.12. tvirtina:

9.12.1.rizikos vertinimo ir rizikos valdymo priemonių planą;

9.12.2.grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinės sistemos kibernetiniam saugumui, rizikos vertinimo (toliau – ryšių ir informacinės sistemos rizikos vertinimas) ataskaitą;

9.12.3.informacinės sistemos informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.13. atlieka kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

10. Informacinės sistemos pagrindinio tvarkytojo funkcijos:

10.1. užtikinti:

10.1.1.informacinės sistemos nepertraukiamą veiklą;

10.1.2.elektroninės informacijos saugą, kibernetinį saugumą ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

10.1.3.informacinės sistemos sąveiką su susijusiais registrais ir susijusiomis informacinėmis sistemomis;

10.2. rengti ir įgyvendinti techninių ir programinių priemonių kūrimo ir plėtros planus, investicinius projektus;

10.3. organizuoti naudotojams mokomuosius ir pažintinius kursus elektroninės informacijos tvarkymo klausimais;

10.4. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

11. Informacinės sistemos tvarkytojų funkcijos ir atsakomybė:
    11.1. juridinių asmenų atveju, paskiria savo institucijoje informacinės sistemos naudotojus ir duomenis apie juos pateikia informacinės sistemos administratoriui;
    11.2. institucijose, kuriose yra įdiegtos lokalios informacinės sistemos tarnybinės stotys, paskiria darbuotojus, atsakingus už lokalių informacinės sistemos tarnybinių stočių priežiūrą ir jų tinkamą naudojimą;
    11.3. užtikrina į informacinės sistemos duomenų bazes pateikiamų duomenų tinkamą įvedimą, duomenų teisingumą, saugumą ir konfidencialumą savo įstaigoje ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu) į informacinės sistemos duomenų bazes;
    11.4. užtikrina informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;
    11.5. teikia pasiūlymus informacinės sistemos valdytojui dėl elektroninės informacijos saugos tobulinimo.
12. Už elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją atsako informacinės sistemos valdytojas, pagrindinis tvarkytojas ir tvarkytojai.
13. Informacinės sistemos pagrindinis tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos dokumentuose nustatyta tvarka.
14. Saugos įgaliotinio funkcijos:
    14.1. teikti informacinės sistemos pagrindinio tvarkytojo vadovui pasiūlymus dėl informacinės sistemos administratorių paskyrimo ir reikalavimų jiems nustatymo;
    14.2. organizuoti informacinių technologijų saugos atitikties vertinimą pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – saugos atitikties vertinimo metodika);
    14.3. teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;
    14.4. koordinuoti elektroninės informacijos saugos ir kibernetinio saugumo incidentų tyrimą, bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinio saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos ir kibernetinio saugumo incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos ar kibernetinio saugumo darbo grupės;
    14.5. teikti informacinės sistemos administratoriams ir naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo;
    14.6. organizuoti rizikos ir informacinių technologijų saugos atitikties vertinimą;
    14.7. atlikti kitas Saugos nuostatuose, kituose teisės aktuose nustatytas ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše saugos įgaliotiniui priskirtas funkcijas.
15. Kibernetinio saugumo vadovas atlieka 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“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas), Nacionaliniame kibernetinių incidentų valdymo plane, 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“ ir kituose teisės aktuose nustatytas funkcijas. Kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

16. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti informacinės sistemos administratoriaus funkcijų.
17. Administratoriai yra šie:
    17.1. informacinės sistemos administratorius (toliau – administratorius) – informacinės sistemos administratorius, atsakingas už informacinės sistemos administravimą, klasifikavimo sistemų valdymą, duomenų mainų ir archyvavimo komponentes;
    17.2. informacinės sistemos lokalios tarnybinės stoties administratoriai (toliau – LIMIS-M administratoriai) – lokalios tarnybinės stoties administratorius, atsakingas už lokalios tarnybinės stoties administravimą, duomenų valdymą, paieškos ir duomenų teikimo komponentes.
18. Administratoriaus funkcijos ir atsakomybės:
    18.1. pagal kompetenciją registruoja informacinės sistemos tvarkytojus, jų įgaliotus asmenis, informacinės sistemos naudotojus, duomenų gavėjus, suteikia jiems prieigos teises;
    18.2. stabdo informacinės sistemos duomenų tvarkymo ir naudojimo įgaliojimus jų netekusiems asmenims ir informacinės sistemos tvarkytojų įgaliojimus baigus galioti informacinės sistemos tvarkytojo sutarčiai su informacinės sistemos valdytoju;
    18.3. pagal kompetenciją atlieka informacinės sistemos priežiūrą;
    18.4. diegia ir atnaujina elektroninės informacijos saugai užtikrinti skirtas priemones bei keičia jų parametrus;
    18.5. dalyvauja atliekant informacinės sistemos tvarkytojams, informacinės sistemos naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;
    18.6. reguliariai (ne rečiau kaip kartą per metus) ir (arba) po kiekvieno informacinės sistemos pokyčio rengia, tikrina (peržiūri) informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius;
    18.7. dalyvauja nustatant informacinės sistemos pažeidžiamas vietas;
    18.8. dalyvauja atliekant informacinės sistemos informacinių technologijų saugos atitikties vertinimą;
    18.9. nedelsiant vykdo saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus dėl informacinės sistemos saugos politikos įgyvendinimo;
    18.10. pagal kompetenciją reaguoja į saugos incidentus ir nuolat teikia saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;
    18.11. informuoja saugos įgaliotinį ir kibernetinio saugumo vadovą apie saugos politiką įgyvendinančių dokumentų pažeidimus, nusikalstamos veiklos požymius, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones;
    18.12. konsultuoja informacinės sistemos tvarkytojus informacinės sistemos tarnybinių stočių priežiūros ir naudojimo klausimais.
    18.13. atsako už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.
19. LIMIS-M administratoriaus funkcijos ir atsakomybės:

19.1. užtikrina kompiuterių tinklų veikimą konkrečioje lokalioje tarnybinėje stotyje;

19.2. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą konkrečioje lokalioje tarnybinėje stotyje;

19.3. reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio patikrina (peržiūri) informacinės sistemos sąranką, būsenos rodiklius konkrečioje lokalioje tarnybinėje stotyje;

19.4. atsako už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.

20. Teisės aktai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą:

20.1. Lietuvos Respublikos muziejų įstatymas;

20.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

20.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1);

20.6. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

20.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. nutarimu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

20.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas;

20.9. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001bei kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugą;

20.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymą, elektroninės informacijos saugą, kibernetinį saugumą bei informacinės sistemos valdytojo ir tvarkytojų veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto 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“ (toliau – Klasifikavimo gairių aprašas), 8.1 , 8.3 ir 8.6 papunkčiais.

22. Informacinė sistema pagal joje tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.2 papunkčiu, priskiriama antrajai kategorijai.

23. Saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“ ir Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja informacinės sistemos rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos vertinimą. Informacinės sistemos pagrindinio tvarkytojo rašytiniu pavedimu informacinės sistemos rizikos vertinimą gali atlikti pats saugos įgaliotinis.
24. Informacinės sistemos rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo vadovui. Rizikos vertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:
    24.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingai pateikta elektroninė informacija, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais triktys, programinės įrangos klaidos ar netinkamas veikimas ir kita);
    24.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);
    24.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure)* aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.
25. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinės sistemos valdytojo vadovas prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.
26. Rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Lietuvos Respublikos krašto apsaugos ministro nustatyta tvarka.
27. Vadovaujantis Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimais, kasmet, arba po esminių organizacinių ar sisteminių pokyčių, organizuojamas Grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimas (toliau – ryšių ir informacinės sistemos rizikos vertinimas). Informacinės sistemos valdytojo vadovo rašytiniu pavedimu ryšių ir informacinės sistemos rizikos vertinimą gali atlikti pats saugos įgaliotinis. Ryšių ir informacinės sistemos rizikos vertinimo metu:
    27.1. paskiriama už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingas asmuo arba asmenys ir nustatomi jiems taikomi kvalifikaciniai reikalavimai;
    27.2. nustatomi reikalavimai rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijai ir priimtinas rizikos lygis;

27.3. nustatomi grėsmės ir pažeidžiamumai, galintys turėti įtakos ryšių ir informacinės sistemos kibernetiniam saugumui, ir nustatomi galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys;

27.4. įvertinama ryšių ir informacinės sistemos pažeidimo grėsmių tikimybė ir pasekmės, nustatomas rizikos lygis, įvertinama identifikuotų grėsmių tikimybes ir jos išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą;

27.5. atsižvelgiant į atliktą rizikos vertinimą, rengiami ir (ar) peržiūrimi patvirtinti teisės aktai, reglamentuojantys informacinės sistemos kibernetinio saugumo politiką ir jos įgyvendinimą.

28. Organizuojant ryšių ir informacinės sistemos rizikos vertinimą, rekomenduojama vadovautis Lietuvos ir tarptautiniais standartais ar metodikomis, reglamentuojančiais rizikos valdymą.

29. Ryšių ir informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinės sistemos rizikos vertinimu ar informacinės sistemos informacinių technologijų saugos atitikties vertinimu.

30. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo organizavimą ir kontrolę, turi būti organizuojami informacinės sistemos informacinių technologijų saugos atitikties vertinimai:

30.1. informacinės sistemos informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

30.2. informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

31. Informacinės sistemos saugos atitikties vertinimas atliekamas saugos atitikties vertinimo metodikoje nustatyta tvarka.

32. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis rengia ir informacinės sistemos valdytojo vadovui teikia informacinių technologijų saugos atitikties vertinimo ataskaitą. Atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.

33. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Lietuvos Respublikos krašto apsaugos ministro nustatyta tvarka.

34. Siekiant gerinti elektroninės informacijos saugos ir kibernetinio saugumo būklę, techninės, programinės, organizacinės ir kitos elektroninės informacijos saugos ir kibernetinio saugumo priemonės pasirenkamos atsižvelgiant į informacinės sistemos valdytojo turimus išteklius ir vadovaujantis šiais principais:

34.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

34.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

34.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos ir kibernetinio saugumo priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

35. Informacinėje sistemoje naudojamų interneto viešųjų prieigų (svetainių) saugos valdymo reikalavimai:
    35.1. svetainės turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus;
    35.2. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų būtų galima jungtis tik iš vidinio informacinės sistemos pagrindinio tvarkytojo ar tvarkytojo kompiuterių tinklo arba nustatytų IP adresų;
    35.3. turi būti pakeisti numatytieji (angl. *default*) prisijungimo prie svetainių turinio valdymo sistemų ir administravimo skydų (angl. *panel*) slaptažodžiai ir nuorodos (angl. *default path*);
    35.4. turi būti užtikrinama, kad prie svetainių turinio valdymo sistemų ir administravimo skydų būtų galima jungtis tik naudojantis šifruotuoju ryšiu;
    35.5. informacinėje sistemoje naudojamų svetainių sauga turi būti vertinama informacinės sistemos rizikos įvertinimo, ryšių ir informacinės sistemos rizikos vertinimo ir (arba) informacinės sistemos informacinių technologijų saugos atitikties vertinimo, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka, metu.
36. Programinės įrangos, skirtos informacinę sistemą apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:
    36.1. tarnybinėse stotyse ir naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiuoju laiku priemonės;
    36.2. informacinės sistemos komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami tik tuo atveju, jeigu rizikos vertinimo ar ryšių ir informacinės sistemos rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;
    36.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per savaitę. Administratorius arba LIMIS-M administratorius turi būti automatiškai informuojamas elektroniniu paštu apie tai, kurių informacinės sistemos posistemių, funkciškai savarankiškų sudedamųjų dalių, naudotojų kompiuterių ir kitų informacinės sistemos komponentų kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas, ir apie tai, kad kenksmingos programinės įrangos aptikimo priemonės funkcionuoja netinkamai arba yra išjungtos.
37. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:
    37.1. informacinės sistemos tarnybinėse stotyse ir naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga;
    37.2. naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į su informacinės sistemos valdytoju suderintą Leidžiamos naudoti programinės įrangos sąrašą, kurį turi parengti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti saugos įgaliotinis;

37.3. ne rečiau kaip kartą per mėnesį turi būti įvertinami tarnybinių stočių ir naudotojų kompiuterių operacinės sistemos kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami;

37.4. administratorius arba LIMIS-M administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius informacinės sistemos posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, naudotojų kompiuteriuose. Apie įvertinimo rezultatus administratorius ir LIMIS-M administratorius turi informuoti saugos įgaliotinį ir kibernetinio saugumo vadovą;

37.5. programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų;

37.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – administratoriai, LIMIS-M administratoriai arba tokias paslaugas teikiantys paslaugų teikėjai;

37.7. programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje neturi būti naudojami realūs asmens duomenys arba užtikrinamos kitos priemonės saugiam tokių duomenų naudojimui;

37.8. informacinės sistemos programinė įranga turi turėti apsaugą 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.

38. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kt.) pagrindinės naudojimo nuostatos:

38.1. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, apsaugos nuo internetinės paslaugos sutrikdymo atakų ir srautinių internetinės paslaugos sutrikdymo atakų įrangą;

38.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuosiuose ryšių tinkluose naršančių naudotojų kompiuterinę įrangą nuo kenksmingo kodo. Visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

38.3. apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga;

38.4. turi būti naudojamos turinio filtravimo sistemos;

38.5. turi būti naudojamos taikomųjų programų kontrolės sistemos.

39. Leidžiamos kompiuterių naudojimo ribos:

39.1. stacionariuosius kompiuterius leidžiama naudoti tik informacinės sistemos valdytojo ir informacinės sistemos tvarkytojo patalpose;

39.2. nešiojamiesiems kompiuteriams, išnešamiems iš informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimai ir pan.);

39.3. iš stacionariųjų ir nešiojamųjų kompiuterių ar elektroninės informacijos laikmenų, kurie perduodami remonto ar techninės priežiūros paslaugų teikėjui arba nurašomi, turi būti nebeatkuriamai pašalinta visa nevieša elektroninė informacija.

40. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:
    40.1. elektroninė informacija teikiama informacinės sistemos nuostatuose, patvirtintuose Lietuvos dailės muziejaus direktoriaus 2010 m. vasario 26 d. įsakymu Nr. V.1-25 „Dėl Lietuvos integralios muziejų informacinės sistemos (LIMIS) nuostatų patvirtinimo“, nustatyta tvarka;
    40.2. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą naudojamas šifravimas, virtualusis privatusis tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Elektroninės informacijos teikimui ir (ar) gavimui gali būti naudojamas saugus valstybinis duomenų perdavimo tinklas;
    40.3. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal Informacinės sistemos nuostatuose, elektroninės informacijos teikimo (keitimosi ja) sutartyse nustatytas specifikacijas ir sąlygas;
    40.4. nuotolinis prisijungimas prie informacinės sistemos galimas:
        40.4.1. naudojant transporto lygmens protokolus (TLS), reglamentuojančius abipusį tapatumo nustatymą tarp naudotojo ir serverio, kad būtų užtikrintas šifruotasis ryšys. Saugiam elektroninės informacijos perdavimui tarp serverio ir interneto naršyklės naudojamas TLS sertifikatas, patvirtinantis elektroninės informacijos šaltinio tapatumą ir šifruojantis tarp naudotojo ir serverio siunčiamą elektroninę informaciją. Informacinės sistemos interneto svetainėse TLS šifruota HTTP protokolo elektroninė informacija perduodama saugiu HTTPS protokolu;
        40.4.2. naudojant virtualųjį privatųjį tinklą (virtualiajame tinkle turi būti naudojamas IPsec protokolų rinkinys);
        40.4.3. naudojant saugaus apvalkalo (angl. *Secure Shell*) protokolą ir nuotolinio darbalaukio protokolą (šia galimybe gali būti pasinaudota tik informacinės sistemos administravimo tikslais);
    40.5. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai bei kiti šifravimo algoritmai turi būti nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų bei standartų rekomendacijas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus, Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus;
    40.6. naudojamų šifravimo priemonių patikimumas turi būti vertinamas atliekant neeilinį arba kasmetinį informacinės sistemos rizikos vertinimą ar ryšių ir informacinės sistemos rizikos vertinimą. Šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.
41. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:
    41.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą ir priimtiną informacinės sistemos neveikimo laikotarpį;
    41.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad informacinės sistemos veiklos sutrikimo, elektroninės informacijos saugos ar kibernetinio incidento arba elektroninės informacijos vientisumo praradimo atvejais informacinės sistemos neveikimo laikotarpis nebūtų ilgesnis, nei numatytas antros

kategorijos informacinei sistemai, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

41.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai ir periodiškai;

41.4. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių neteisėtai atkurti elektroninės informacijos;

41.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose, nei yra informacinės sistemos tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

41.6. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

41.7. periodiškai, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

41.8. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

42. Informacinės sistemos valdytojas ir (arba) informacinės sistemos tvarkytojas, pirkdamas paslaugas, darbus ar prekes, susijusias su informacine sistema, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Naudotojų, administratorių, LIMIS-M administratorių, saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacijos ir patirties reikalavimai:

43.1. naudotojų, administratorių, LIMIS-M administratorių, saugos įgaliotinio, kibernetinio saugumo vadovo kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareiginiuose nuostatuose;

43.2. visi naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų ir elektroninės informacijos tvarkymą. Asmenys, tvarkantys asmens duomenis ir informaciją, privalo būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį ir jo laikytis. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

43.3. saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti elektroninės informacijos saugos ir kibernetinio saugumo srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą ir kibernetinį saugumą. Informacinės sistemos valdytojas turi sudaryti sąlygas kelti saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikaciją;

43.4. saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinės sistemos saugumui, paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, už savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo yra praėję mažiau kaip vieni metai;

43.5. administratoriai ir LIMIS-M administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą, administruoti ir prižiūrėti informacinės sistemos komponentus (stebėti informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Administratoriai ir LIMIS-M administratoriai turi būti susipažinę su saugos dokumentais.

44. Saugos įgaliotinio, kibernetinio saugumo vadovo, naudotojų, LIMIS-M administratorių ir administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

44.1. saugos įgaliotiniui, kibernetinio saugumo vadovui, naudotojams, LIMIS-M administratoriams ir administratoriams turi būti organizuojami mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais;

44.2. naudotojams turi būti įvairiais būdais (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems naudotojams ir administratoriams ir pan.) primenama apie elektroninės informacijos saugos ar kibernetinio saugumo problemas;

44.3. mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į prioritetines elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, kibernetinio saugumo vadovo, naudotojų, LIMIS-M administratorių ar administratorių poreikius;

44.4. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

44.5. naudotojų, LIMIS-M administratorių ir administratorių mokymus organizuoja saugos įgaliotinis. Mokymus gali vykdyti saugos įgaliotinis ar kitas informacinės sistemos valdytojo darbuotojas, išmanantis elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, arba elektroninės informacijos saugos ir kibernetinio saugumo mokymų paslaugų teikėjas. Saugos įgaliotinio ir kibernetinio saugumo vadovo mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos ir kibernetinio saugumo mokymų paslaugų teikėjas;

44.6. naudotojų mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per metus. Saugos įgaliotinio, kibernetinio saugumo vadovo, LIMIS-M administratorių ir administratorių mokymai turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

45. Naudotojų supažindinimą su saugos dokumentais, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis.
46. Informacinės sistemos naudotojų supažindinimo su saugos dokumentais ar jų santrauka būdai turi būti pasirenkami atsižvelgiant į informacinės sistemos specifiką (pvz., informacinės sistemos ir jos naudotojų lokaciją, organizacinių ar techninių priemonių, leidžiančių identifikuoti su saugos dokumentais susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.). Naudotojai su saugos dokumentais ar jų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.
47. Pakartotinai su saugos dokumentais ar jų santrauka naudotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojantiems teisės aktams.
48. Tvarkyti elektroninę informaciją gali tik tie asmenys, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų.
49. Naudotojai atsako už informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal savo kompetenciją. Naudotojai, LIMIS-M administratoriai, administratoriai, kibernetinio saugumo vadovas ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Lietuvos Respublikos krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką. Keičiami saugos dokumentai gali būti nederinami su Lietuvos Respublikos krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba pakeitimai, susiję su teisės technika.
51. Patvirtinęs Saugos nuostatus ar jų pakeitimus, informacinės sistemos valdytojas Registrų ir valstybės informacinių sistemų registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimu Nr. 1263 „Dėl Registrų sąrašo reorganizavimo į Registrų ir valstybės informacinių sistemų registrą ir Registrų ir valstybės informacinių sistemų registro nuostatų patvirtinimo“, nustatyta tvarka pateikia šiam registrui reikiamus duomenis ar dokumentų kopijas.
52. Patvirtintų saugos dokumentų ir jų pakeitimų kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Lietuvos Respublikos krašto apsaugos ministro nustatyta tvarka.

53. Informacinės sistemos valdytojas saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos vertinimą, ryšių ir informacinės sistemos rizikos vertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems informacinės sistemos valdytojo pokyčiams.

_____

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