LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTRAS

ĮSAKYMAS
DĖL MOKINIŲ UGDYMO KARJERAI INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2024 m. spalio 25 d. Nr. V-1196
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 5 punktu, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, 19 ir 26 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunkčiu:

1. T v i r t i n u Mokinių ugdymo karjerai informacinės sistemos duomenų saugos nuostatus (pridedama).

2. P a v e d u Lietuvos neformaliojo švietimo agentūrai:

2.1. per vieną mėnesį nuo Mokinių ugdymo karjerai informacinės sistemos duomenų saugos nuostatų patvirtinimo paskirti Mokinių ugdymo karjerai informacinės sistemos saugos įgaliotinį ir administratorių;

2.2. per tris mėnesius nuo Saugos nuostatų patvirtinimo parengti ir pateikti Lietuvos Respublikos švietimo, mokslo ir sporto ministrui tvirtinti Mokinių ugdymo karjerai informacinės sistemos saugos politiką įgyvendinančių dokumentų projektus.

3. S k i r i u Lietuvos neformaliojo švietimo agentūrą atsakinga už Mokinių ugdymo karjerai informacinės sistemos kibernetinio saugumo organizavimą ir užtikrinimą.

Švietimo, mokslo ir sporto ministrė Radvilė Morkūnaitė-Mikulėnienė

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2024 m. liepos 3 d. raštu Nr. (4,1E)6K-478

PATVIRTINTA
Lietuvos Respublikos švietimo,
mokslo ir sporto ministro
2024 m. spalio 25 d.
įsakymu Nr. V-1196

MOKINIŲ UGDYMO KARJERAI INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Mokinių ugdymo karjerai informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos (toliau – ŠMSM) valdomos bei Lietuvos neformaliojo švietimo agentūros (toliau – LINEŠA) tvarkomos Mokinių ugdymo karjerai informacinės sistemos (toliau – MUKIS) elektroninės informacijos saugos ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. MUKIS elektroninės informacijos saugos politika įgyvendinama pagal švietimo, mokslo ir sporto ministro tvirtinamus MUKIS saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau – saugos politiką įgyvendinantys dokumentai). Saugos nuostatuose vartojamos sąvokos atitinka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (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) (toliau – Reglamentas), Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Bendrųjų saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

3. MUKIS elektroninės informacijos sauga – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

4. MUKIS elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, praradimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevenciją.

5. MUKIS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. elektroninės informacijos tvarkymo ir jos naudojimo kontrolė;

5.2. elektroninės informacijos tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

5.3. MUKIS tvarkomų asmens duomenų apsauga;

5.4. MUKIS veikos tęstinumo užtikrinimas.

6. MUKIS elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

7. Saugos nuostatų reikalavimai taikomi:

7.1. MUKIS valdytojui – ŠMSM, A. Volano g. 2, Vilnius;

7.2. MUKIS tvarkytojui – LINEŠA, Žirmūnų g. 1B, Vilnius;

7.3. MUKIS tvarkytojo paskirtam saugos įgaliotiniui – darbuotojui, dirbančiam pagal darbo sutartį, koordinuojančiam ir prižiūrinčiam saugos politikos įgyvendinimą MUKIS;

7.4. MUKIS administratoriui – darbuotojui, dirbančiam pagal darbo sutartį, prižiūrinčiam MUKIS ir (ar) jos infrastuktūrą, užtikrinančiam jos veikimą ir elektroninės informacijos saugą, ar kitam asmeniui (asmenų grupei), kuriam Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka yra perduotos MUKIS ir (ar) jos infrastuktūros priežiūros funkcijos;

7.5. MUKIS naudotojams – darbuotojams, dirbantiems pagal darbo sutartį, ar kitiems asmenims, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantiems ir (ar) tvarkantiems elektroninę informaciją;

7.6. paslaugų, susijusių su MUKIS, teikėjams.

8. Už elektroninės informacijos saugą pagal kompetenciją atsako MUKIS valdytojas ir tvarkytojas.

9. MUKIS valdytojas atsako už MUKIS elektroninės informacijos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą, elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo duomenų gavėjams teisėtumą. MUKIS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

10. MUKIS naudotojai, tvarkantys duomenis, informaciją, dokumentus ir (arba) jų kopijas, privalo įsipareigoti saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymu susijusią veiklą.

11. Paslaugų, susijusių su MUKIS, teikėjai privalo įsipareigoti saugoti duomenų ir informacijos paslaptį bei pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

12. MUKIS valdytojas atlieka MUKIS nuostatuose nustatytas funkcijas, o taip pat:

12.1. tvirtina Saugos nuostatus, saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga;

12.2. prižiūri ir kontroliuoja, kad MUKIS būtų tvarkomos vadovaujantis MUKIS nuostatais, Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais duomenų saugą reglamentuojančiais teisės aktais;

12.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

12.4. tvirtina MUKIS rizikos įvertinimo ir rizikos valdymo priemonių planą ir informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą; esant poreikiui šie planai gali būti sujungti ir tvirtinamas bendras planas;

12.5. koordinuoja MUKIS tvarkytojo darbą įgyvendinant elektroninės informacijos saugos reikalavimus;

12.6. nagrinėja MUKIS tvarkytojo pasiūlymus dėl MUKIS elektroninės informacijos saugos priemonių tobulinimo ir priima dėl jų sprendimus;

12.7. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, MUKIS nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

13. MUKIS tvarkytojas atlieka MUKIS nuostatuose nustatytas funkcijas, o taip pat:

13.1. užtikrina elektroninės informacijos, esančios MUKIS duomenų bazėse, saugą;

13.2. užtikrina saugią MUKIS sąveiką su kitomis informacinėmis sistemomis ir registrais;

13.3. užtikrina tinkamą Saugos nuostatų, MUKIS saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

13.4. rengia MUKIS rizikos įvertinimo ir rizikos valdymo priemonių planą ir informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą; esant poreikiui šie planai gali būti sujungti ir rengiamas bendras planas;

13.5. teikia siūlymus MUKIS valdytojui dėl MUKIS elektroninės informacijos saugos tobulinimo, MUKIS saugos dokumentų priėmimo, keitimo arba panaikinimo, MUKIS techninių ir programinių priemonių, būtinų MUKIS elektroninės informacijos saugai užtikrinti;

13.6. atlieka MUKIS techninę priežiūrą ir užtikrina nepertraukiamą MUKIS veikimą;

13.7. skiria MUKIS saugos įgaliotinį bei MUKIS administratorių, paveda jiems atlikti funkcijas nustatytas MUKIS nuostatuose, MUKIS saugos politiką įgyvendinančiuose dokumentuose;

13.8. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose;

13.9. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, MUKIS nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

14. MUKIS tvarkytojo paskirtas saugos įgaliotinis atlieka šias funkcijas:

14.1. teikia MUKIS tvarkytojo vadovui pasiūlymus dėl:

14.1.1. MUKIS administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

14.1.2. informacinių technologijų saugos atitikties vertinimo atlikimo;

14.1.3. saugos dokumentų priėmimo ir (ar) keitimo;

14.2. koordinuoja ir prižiūri MUKIS saugos politikos įgyvendinimą;

14.3. supažindina su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą MUKIS tvarkytojo naudotojus;

14.4. rengia MUKIS saugos dokumentus, teikia MUKIS valdytojui siūlymus dėl Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo ir keitimo;

14.5. kasmet organizuoja saugos mokymus, reguliariai primena saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir kt. būdais), prireikus rengia atmintines MUKIS tvarkytojo naudotojams;

14.6. koordinuoja elektroninės informacijos saugos incidentų, įvykusių MUKIS, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis tokius incidentus ir neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

14.7. informuoja MUKIS valdytoją ir kompetentingas institucijas apie neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią MUKIS saugą;

14.8. informuoja už kibernetinio saugumo organizavimą ir užtikrinimą LINEŠA atsakingą asmenį (toliau – už kibernetinį saugumą atsakingas asmuo) apie kibernetinio saugumo incidentus;

14.9. teikia MUKIS naudotojams ir MUKIS administratoriui privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

14.10. pagal kompetenciją kitiems MUKIS valdytojo ir tvarkytojo darbuotojams duoda privalomus vykdyti nurodymus ir pavedimus, būtinus saugos politikai įgyvendinti;

14.11. atlieka pats arba organizuoja MUKIS saugos rizikos įvertinimo procedūras;

14.12. rengia ir ne rečiau kaip kartą per metus peržiūri autorizuotų nuotoliniam prisijungimui MUKIS naudotojų sąrašą;

14.13. ne rečiau kaip kartą per metus organizuoja kompiuterių tinklo užkardų sąrankos peržiūrą;

14.14. atlieka kitas MUKIS tvarkytojo vadovo ar jo įgalioto asmens pavestas, Saugos nuostatuose ir MUKIS saugos politiką įgyvendinančiuose dokumentuose jam nustatytas funkcijas.

15. MUKIS administratoriaus funkcijos:

15.1. atsako už nepertraukiamą MUKIS veikimą;

15.2. administruoja prieigos prie MUKIS teises;

15.3. stebi ir įvertina MUKIS ir MUKIS sudedamųjų dalių (tarnybinių stočių (programų, duomenų bazių valdymo sistemų), kompiuterių tinklo programinės ir duomenų perdavimo įrangos) sąrankos (kaip vienos visumos) veikimą, būklės rodiklius, nustato MUKIS pažeidžiamas vietas; ne rečiau kaip kartą per metus ir (ar) įdiegus MUKIS pokyčius patikrina (peržiūri) MUKIS sąranką ir MUKIS būsenos rodiklius;

15.4. tvarko MUKIS elektroninių duomenų archyvą ir elektroninių duomenų perkėlimo įrašų žurnalą;

15.5. dalyvauja atkuriant MUKIS elektroninius duomenis iš duomenų archyvo;

15.6. tvarko MUKIS techninę dokumentaciją ir eksploatavimo žurnalą;

15.7. pagal kompetenciją dalyvauja atliekant MUKIS saugos atitikties ir (ar) rizikos įvertinimo procedūras;

15.8. teikia pasiūlymus MUKIS saugos įgaliotiniui ir už kibernetinį saugumą atsakingam asmeniui dėl MUKIS saugos organizavimo, atlieka kitas Saugos nuostatuose ir kituose saugos dokumentuose nustatytas funkcijas;

15.9. pagal kompetenciją teikia MUKIS tvarkytojo vadovui siūlymus dėl MUKIS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

15.10. registruoja elektroninės informacijos saugos incidentus ir informuoja apie juos MUKIS saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

15.11. įvertina MUKIS naudotojų pasirengimą dirbti su MUKIS, konsultuoja juos, kaip dirbti su MUKIS;

15.12. atlieka kitas MUKIS tvarkytojo vadovo, MUKIS saugos įgaliotinio pavestas, Saugos nuostatuose ir MUKIS saugos politiką įgyvendinančiuose dokumentuose jam nustatytas funkcijas.

16. MUKIS administratorius privalo vykdyti saugos įgaliotinio ir (ar) už kibernetinį saugumą atsakingo asmens nurodymus ir pavedimus dėl MUKIS elektroninės informacijos saugos ir (ar) kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į saugos ir (ar) kibernetinius incidentus, juos valdyti ir nuolat teikti saugos įgaliotiniui ir (ar) už kibernetinį saugumą atsakingam asmeniui informaciją apie saugą užtikrinančių pagrindinių MUKIS sudedamųjų dalių būklę.

17. MUKIS tvarkytojo paskirtas saugos įgaliotinis negali atlikti MUKIS administratoriaus funkcijų.

18. MUKIS naudotojų funkcijos:

18.1. vadovaudamiesi Saugos nuostatais, MUKIS naudojimo instrukcijomis ir pareigybių aprašymais, naudoja MUKIS;

18.2. tvarko MUKIS elektroninę informaciją ir naudojasi kitomis MUKIS teikiamomis galimybėmis pagal nustatytą funkcijoms atlikti reikalingą MUKIS prieigos teisių lygmenį, kuris apriboja naudojimosi elektronine informacija apimtį;

18.3. pagal kompetenciją rengia pasiūlymus dėl MUKIS kūrimo, palaikymo, priežiūros ir elektroninės informacijos saugos;

18.4. vykdo kitas šiuose Saugos nuostatuose ir Saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas.

19. Teisės aktai, kuriais vadovaujantis tvarkoma MUKIS elektroninė informacija ir užtikrinama jos sauga:

19.1. Reglamentas;

19.2. Valstybės informacinių išteklių valdymo įstatymas;

19.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

19.4. Kibernetinio saugumo įstatymas;

19.5. Bendrųjų saugos reikalavimų aprašas;

19.6. Kibernetinio saugumo reikalavimų aprašas;

19.7. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Atitikties vertinimo metodika);

19.8. Lietuvos standartai LST ISO/IEC 27001:2017 ir LST ISO/IEC 27002:2017 bei Lietuvos ir tarptautiniai „Informacijos technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

19.9. Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo patvirtinimo“ (toliau – Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašas);

19.10. 2023 m. liepos 19 d. Lietuvos Respublikos Vyriausybės nutarimas Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“ (toliau – Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašas);

19.11. MUKIS nuostatai, Saugos nuostatai, MUKIS saugos politiką įgyvendinantys dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Remiantis Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašu, MUKIS priskiriama vidutinės svarbos valstybės informacinių išteklių rūšiai.

21. MUKIS rizikos įvertinimas atliekamas vadovaujantis šiomis nuostatomis:

21.1. MUKIS rizikos įvertinimas atliekamas ne rečiau kaip kartą per metus, jeigu teisės aktuose nenustatyta kitaip;

21.2. neeilinis MUKIS rizikos įvertinimas atliekamas padarius esminius MUKIS funkcinius pakeitimus arba kai atsiranda naujų informacinių technologijų saugos srities reikalavimų, arba po didelio masto saugos ir (ar) kibernetinių incidentų, kai nustatoma naujų rizikos formų;

21.3. rizikos veiksniams įvertinti naudojama kokybinė rizikos vertinimo sistema vadovaujantis metodika, pateikta Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamame Rizikos analizės vadove, Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais.

22. MUKIS saugos įgaliotinis organizuoja MUKIS rizikos vertinimą, kuriam atlikti sutartiniais pagrindais gali būti samdomi tretieji asmenys.

23. Įdiegus MUKIS pokyčius (sistemos pakeitimai, konfigūracijų pakeitimai, programinės įrangos versijų naujinimas, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) arba atlikus esminius organizacinius ar sisteminius pokyčius ir nustačius naujus rizikos veiksnius, gali būti organizuojamas neeilinis MUKIS rizikos vertinimas.

24. MUKIS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri teikiama MUKIS valdytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinus rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

25. Atsižvelgdamas į rizikos vertinimo ataskaitą, MUKIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano duomenis bei jų kopijas MUKIS saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo šių

dokumentų patvirtinimo pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą (toliau – ARSIS).

27. MUKIS informacinių technologijų saugos atitikties vertinimas atliekamas Atitikties vertinimo metodikoje nustatyta tvarka.

28. Informacinių technologijų saugos atitikties vertinimo organizavimas:

28.1. siekiant užtikrinti MUKIS saugos dokumentuose nustatytų MUKIS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas;

28.2. informacinių technologijų saugos atitikties vertinimas atliekamas Atitikties vertinimo metodikoje nustatyta tvarka;

28.3. atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama MUKIS valdytojo ir MUKIS tvarkytojo vadovams;

28.4. atlikus informacinių technologijų saugos atitikties vertinimą, prireikus rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus plano vykdytojus paskiria ir įgyvendinimo terminus nustato MUKIS valdytojo vadovas.

29. MUKIS informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas MUKIS saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo pateikia ARSIS.

30. MUKIS informacinių technologijų saugos priemonės parenkamos įvertinus galimus rizikos elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui veiksnius.

31. Elektroninės informacijos saugos ir kibernetinio saugumo būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis elektroninės informacijos saugos ir kibernetinio saugumo priemonėmis. Šios priemonės pasirenkamos atsižvelgiant į MUKIS valdytojo turimus išteklius, vadovaujantis šiais principais:

31.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

31.2. priemonės kaštai neturi viršyti žalos vertės;

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

32. Ne rečiau kaip kartą per trejus metus MUKIS informacinių technologijų saugos reikalavimų atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo reikalavimai:

33.1. MUKIS tarnybinėse stotyse ir MUKIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga;

33.2. MUKIS darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į leistinos programinės įrangos sąrašą, patvirtintą LINEŠA vadovo įsakymu. Leistinos programinės įrangos sąrašą turi parengti ir pagal poreikį peržiūrėti bei prireikus atnaujinti MUKIS saugos įgaliotinis kartu su administratoriumi;

33.3. tarnybinių stočių ir MUKIS 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;

33.4. MUKIS administratorius reguliariai, ne rečiau kaip kartą per mėnesį, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir jų įtaką MUKIS

pažeidžiamumui. Apie įvertinimo rezultatus MUKIS administratorius turi informuoti MUKIS saugos įgaliotinį;

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

33.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – MUKIS administratorius arba tokias paslaugas teikiantys kvalifikuoti paslaugų teikėjai.

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

34.1. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

34.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuosiuose ryšių tinkluose naršančių vidinių informacinių sistemų 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;

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

35. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

35.1. prieiga prie MUKIS suteikiama tik registruotiems MUKIS naudotojams;

35.2. tiesioginė prieiga prie MUKIS elektroninės informacijos suteikiama įgyvendinus MUKIS naudotojų autentifikavimo priemones – šie naudotojai savo tapatybę patvirtina slaptažodžiu ar kita autentifikavimo priemone;

35.3. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, naudojamas šifravimas, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas;

35.3. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal MUKIS nuostatuose, duomenų teikimo sutartyse nustatytas sąlygas ir specifikacijas.

36. Saugos valdymo reikalavimai, keliami išorinei MUKIS svetainei:

36.1. svetainė turi atitikti Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms apraše bei Kibernetinio saugumo reikalavimų apraše nurodytiems reikalavimams;

36.2. svetainės užkarda turi būti sukonfigūruota taip, kad prie turinio valdymo sistemos (toliau – TVS) būtų galima jungtis tik iš MUKIS tvarkytojo vidinio kompiuterių tinklo arba nustatytų kompiuterio adresų (angl. *Internet Protocol*);

36.3. turi būti užtikrinama, kad prie TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotuoju ryšiu.

37. Programinės įrangos, skirtos MUKIS apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

37.1. tarnybinėse stotyse ir MUKIS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiuoju laiku priemonės;

37.2. MUKIS komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti naudojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina;

37.3. MUKIS administratorius turi būti automatiškai informuojamas apie tai, kurių MUKIS naudotojų kompiuterių ar MUKIS aptarnaujančios infrastruktūros serverių kenksmingos programinės įrangos aptikimo priemonių atsinaujinimas pradelstas nepriimtinai, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos;

37.4. MUKIS administratorius turi būti automatiškai elektroniniu paštu informuojamas apie tai, kurių MUKIS posistemių, funkciškai savarankiškų MUKIS sudedamųjų dalių ir (ar) kitų MUKIS

sudedamųjų dalių kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

38. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

38.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objective*) ir priimtiną MUKIS neveikimo laikotarpį (angl. *recovery time objective*);

38.2. MUKIS elektroninės informacijos kopijos saugomos kitoje patalpoje nei tarnybinės stotys;

38.3. atsarginių elektroninės informacijos kopijų darymo tvarka ir saugojimo terminai nustatomi MUKIS tvarkytojo vadovo įsakymu tvirtinamame atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkos apraše (toliau – Atsarginių kopijų aprašas); apie sutrikusias atsarginių kopijų darymo procedūras informuojamas MUKIS saugos įgaliotinis;

38.4. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau kaip Atsarginių kopijų apraše nurodytais terminais;

38.5. atsarginės elektroninės informacijos kopijos turi būti tvarkomos taip, kad net ir praradus pagrindinį MUKIS duomenų centrą būtų užtikrinami priimtini atkūrimo taško (angl. *recovery point objective*, RPO) ir atkūrimo laiko (angl. *recovery time objective*, RTO) reikalavimai, siekiant maksimaliai sumažinti prastovos laiką ir duomenų praradimo riziką;

38.6. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

38.7. periodiškai, bet ne rečiau kaip kartą per metus, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

38.8. patekimas į patalpas, kuriose veikia MUKIS įranga ir saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

39. MUKIS tarnybinės stotys ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne trumpiau kaip 30 minučių.

40. MUKIS naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie MUKIS galimybė:

40.1. techninis nuotolinio prisijungimo sprendimas turi užtikrinti elektroninės informacijos šifravimą naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN);

40.2. prie MUKIS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

41. MUKIS funkcionalumo atkūrimo ir prieinamumo reikalavimai:

41.1. pagrindinės MUKIS funkcijos turi būti atkurtos per 12 valandų nuo veiklos sutrikimo;

41.2. turi būti užtikrintas galimas ne didesnis kaip 4 valandų darbo laiko duomenų praradimas;

41.3. turi būti užtikrintas ne mažesnis kaip 96 procentų laiko visą parą MUKIS prieinamumas.

42. Perkant paslaugas, darbus ar įrangą, susijusius su MUKIS priežiūra, modernizavimu, modifikavimu ir (ar) kibernetinio saugumo užtikrinimu, MUKIS tvarkytojo pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas privalo laikytis MUKIS saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų saugos reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą ir kibernetinį saugumą, privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

44. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat 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, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėjo mažiau kaip vieni metai.

45. MUKIS administratorius privalo išmanyti pagrindinius elektroninės informacijos saugos ir saugaus darbo su duomenų perdavimo tinklais principus, atsižvelgiant į atliekamas funkcijas atitinkamai turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą, turėti sisteminių programinių priemonių (*Windows*, *Unix*, *Oracle*) administravimo ir priežiūros patirties.

46. MUKIS naudotojai turi būti susipažinę su Saugos nuostatais, saugos politikos įgyvendinimo dokumentais, pagal kompetenciją – ir su kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

47. MUKIS naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti MUKIS administratoriui ir (ar) MUKIS saugos įgaliotiniui.

48. MUKIS naudotojai privalo:

48.1. turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti saugiai tvarkyti elektroninę informaciją;

48.2. nuolat kelti kvalifikaciją saugaus elektroninės informacijos tvarkymo kursuose, mokymuose, seminaruose;

48.3. praradę arba kitaip netekę savo prisijungimo prie MUKIS vardo ar slaptažodžio, nedelsdami elektroniniu paštu arba telefonu apie tai informuoti MUKIS administratorių.

49. MUKIS naudotojams draudžiama:

49.1. atskleisti kitiems asmenims prisijungimo prie MUKIS vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

49.2. naudoti MUKIS duomenis kitokiais, negu jų nuostatuose nurodytais, ir savo pareigybės aprašyme nustatytų funkcijų atlikimo tikslais;

49.3. sudaryti sąlygas pasinaudoti darbui su MUKIS naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

49.4. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti MUKIS duomenys, taip pat neatlikti būtinų veiksmų, apsaugančių informacinės sistemos duomenis;

49.5. atlikti bet kokius kitus neteisėtus MUKIS duomenų tvarkymo veiksmus.

50. MUKIS naudotojams ne rečiau kaip kartą per kalendorinius metus MUKIS saugos įgaliotinis turi surengti mokymus elektroninės informacijos saugos ir kibernetinio saugumo klausimais, įvairiais būdais priminti apie saugos problemas (pvz., siųsti priminimus elektroniniu paštu, rengti teminius seminarus, atmintines ir pan.).

51. Mokymai MUKIS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas saugos įgaliotinis.

52. Mokymai MUKIS saugos įgaliotiniui ir administratoriui turi būti organizuojami pagal poreikį.

V SKYRIUS
MUKIS NAUDOTOJŲ IR ADMINISTRATORIAUS SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

53. Tvarkyti MUKIS elektroninę informaciją gali tik su Saugos nuostatais, saugos politikos įgyvendinimo dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant MUKIS elektroninę informaciją, užtikrinant jos saugą, susipažinę ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų MUKIS naudotojai.

54. MUKIS naudotojų ir administratoriaus supažindinimą su Saugos nuostatais ir MUKIS saugos politikos įgyvendinimo dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą, atlieka MUKIS saugos įgaliotinis.

55. MUKIS naudotojai ir administratorius pakartotinai su saugos dokumentais supažindinami iš esmės pasikeitus saugos dokumentams ir (arba) padažnėjus elektroninės informacijos saugos incidentų.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

56. Saugos įgaliotinis organizuoja MUKIS saugos dokumentų peržiūrą ne rečiau kaip kartą per metus. Saugos dokumentai turi būti peržiūrimi atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą, įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

57. MUKIS Saugos nuostatų privalo laikytis MUKIS naudotojai, MUKIS administratorius, MUKIS saugos įgaliotinis ir MUKIS duomenų tvarkytojai.

58. MUKIS naudotojai, MUKIS administratorius ir MUKIS saugos įgaliotinis pagal savo kompetenciją atsako už MUKIS tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą. MUKIS naudotojai, MUKIS administratorius ir MUKIS saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

_____