LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTRO ĮSAKYMAS

DĖL KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2025 m. sausio 16 d. Nr. V-37
Vilnius

(TAR, 2025 01 16, Identifikacinis kodas 2025-00456)

Vadovaudamasi Informacinių sistemų steigimo, kūrimo, atnaujinimo, pertvarkymo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimu Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo“, 13 punktu ir Kibernetinio saugumo reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo:

1. T v i r t i n u pridedamus:

1.1. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisykles;

1.3. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planą.

2. N u s t a t a u, kad šio įsakymo 1 punktu patvirtinti dokumentai galioja Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų sąrašui, nurodytam šio įsakymo priede.

3. P r i p a ž į s t u netekusiais galios:

3.1. Lietuvos Respublikos švietimo ir mokslo ministro 2017 m. birželio 12 d. įsakymą Nr. V-470 „Dėl Švietimo ir mokslo institucijų registro saugaus elektroninės informacijos tvarkymo taisyklių, Švietimo ir mokslo institucijų registro naudotojų administravimo taisyklių ir Švietimo ir mokslo institucijų registro veiklos tęstinumo valdymo plano patvirtinimo“;

3.2. Lietuvos Respublikos švietimo ir mokslo ministro 2017 m. liepos 28 d. įsakymą Nr. V-611 „Dėl Studijų, mokymo programų ir kvalifikacijų registro saugaus elektroninės informacijos tvarkymo taisyklių, Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisyklių ir Studijų, mokymo programų ir kvalifikacijų registro veiklos tęstinumo valdymo plano patvirtinimo“;

3.3. Lietuvos Respublikos švietimo ir mokslo ministro 2017 m. birželio 26 d. įsakymą Nr. V-513 „Dėl Mokinių registro saugaus elektroninės informacijos tvarkymo taisyklių, Mokinių registro naudotojų administravimo taisyklių ir Mokinių registro veiklos tęstinumo valdymo plano patvirtinimo“;

3.4. Lietuvos Respublikos švietimo ir mokslo ministro 2018 m. kovo 8 d. įsakymą Nr. V-234 „Dėl Pedagogų registro saugaus elektroninės informacijos tvarkymo taisyklių, Pedagogų registro naudotojų administravimo taisyklių ir Pedagogų registro veiklos tęstinumo valdymo plano patvirtinimo“;

3.5. Lietuvos Respublikos švietimo ir mokslo ministro 2016 m. rugsėjo 13 d. įsakymą Nr. V-777 „Dėl Studentų registro saugaus elektroninės informacijos tvarkymo taisyklių, Studentų registro naudotojų administravimo taisyklių ir Studentų registro veiklos tęstinumo valdymo plano patvirtinimo“;

3.6. Lietuvos Respublikos švietimo ir mokslo ministro 2017 m. rugsėjo 28 d. įsakymą Nr. V-723 „Dėl Nesimokančių vaikų ir mokyklos nelankančių mokinių informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Nesimokančių vaikų ir mokyklos nelankančių mokinių informacinės sistemos naudotojų administravimo taisyklių ir Nesimokančių vaikų ir mokyklos nelankančių mokinių informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“;

3.7. Lietuvos Respublikos švietimo ir mokslo ministro 2017 lapkričio 14 d. įsakymą Nr. V-878 „Dėl Švietimo portalo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Švietimo portalo informacinės sistemos naudotojų administravimo taisyklių ir Švietimo portalo informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“.

Švietimo, mokslo ir sporto ministrė **RAMINTA POPOVIENĖ**

PATVIRTINTA
Lietuvos Respublikos švietimo, mokslo
ir sporto ministro 2025 m. sausio 16 d.
įsakymu Nr. V-37

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Tvarkymo taisyklės) nustato Švietimo, mokslo ir sporto ministerijos kai kurių valdomų ir Nacionalinės švietimo agentūros (toliau – NŠA) tvarkomų registrų ir informacinių sistemų (toliau – RIS) elektroninę informaciją, RIS naudotojų, RIS administratoriaus, RIS saugos įgaliotinių naudojamas technines ir kitas saugos priemones bei atliekamus veiksmus, užtikrinančius saugų RIS techninės, programinės įrangos funkcionavimą, RIS elektroninės informacijos tvarkymą.

II SKYRIUS
SAUGOS PRIEMONIŲ APRAŠYMAS

2. Registro saugos priemonės parenkamos įvertinus galimus rizikos veiksnius RIS elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui. Pasirenkant saugos priemones prioritetas teikiamas toms priemonėms, kurių diegimas duoda didžiausią poveikį ir reikalauja mažiausiai sąnaudų.

3. Kompiuterinės įrangos saugos priemonės:

3.1. RIS tarnybinės stotys, svarbiausi elektroninės informacijos perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų techninė būklė nuolat stebima;

3.2. kompiuterinės įrangos gedimus registruoja RIS priežiūros administratorius;

3.3. RIS tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo mazgai turi įtampos filtrą ir rezervinių maitinimo šaltinių.

4. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

4.1. RIS tarnybinėse stotyse ir RIS naudotojų kompiuterizuotose darbo vietose yra įdiegtos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

4.2. RIS tarnybinėse stotyse naudojama tik legali programinė įranga;

4.3. RIS naudotojų kompiuterizuotose darbo vietose naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

4.4. RIS techninė ir programinė įranga prižiūrima laikantis gamintojų rekomendacijų. Programinės įrangos diegimą, konfigūravimą, atnaujinimą ir šalinimą turi atlikti tik kvalifikuoti specialistai;

4.5. RIS techninės ir programinės įrangos priežiūrą ir gedimų šalinimą atlieka pagal kompetenciją už kompiuterizuotų darbo vietų priežiūrą atsakingi NŠA darbuotojai;

4.6. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką.

5. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

5.1. RIS elektroninės informacijos perdavimo tinklas atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą. Užkardos įvykių žurnalai turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

5.2. visas duomenų srautas į internetą ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

5.3. RIS tarnybinėse stotyse yra įjungtos užkardos, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su RIS funkcionalumu ir administravimu susijusį, duomenų srautą. Ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir šalinamos pastebėtos neatitiktys saugumo reikalavimams;

5.4. viešaisiais ryšių tinklais perduodamos RIS elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones. Prisijungimas prie RIS vykdomas tik šifruotu HTTPS protokolu.

6. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

6.1. RIS tarnybinės stotys įrengtos atskiroje rakinamoje patalpoje. Patalpoje įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų, įrengta oro kondicionavimo ir drėgmės kontrolės įranga;

6.2. į tarnybinių stočių patalpas gali patekti tik už tarnybinių stočių veikimą atsakingi darbuotojai. Kiti asmenys į tarnybinių stočių patalpas gali patekti tik lydimi darbuotojo, turinčio leidimą patekti į tarnybinių stočių patalpas;

6.3. patalpose, kuriose dirba RIS naudotojai, įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

6.4. NŠA pastate veikia patekimo į patalpas kontrolės sistema;

6.5. NŠA pastato aplinka ir tarnybinių stočių patalpa stebima vaizdo kameromis.

7. Kitos priemonės, naudojamos užtikrinti RIS elektroninės informacijos saugą:

7.1. RIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims, atsarginės laikmenos su programine įranga yra saugomos nedegioje spintoje, kitose patalpose, nei yra RIS tarnybinės stotys;

7.2. pagrindinių tarnybinių stočių įvykių žurnaluose (angl. *event log*) registruojami ir ne trumpiau nei 12 mėnesių saugomi duomenys apie RIS tarnybinių stočių bei programinės įrangos įjungimą, išjungimą, perkrovimą, sėkmingus ir nesėkmingus naudotojų ir RIS administratorių prisijungimus ar atsijungimus nuo RIS tarnybinių stočių, RIS programinės įrangos, naudotojų ir (ar) RIS administratorių teisių naudotis RIS ir (ar) tinklo ištekliais pakeitimus, apie visus naudotojų vykdomus veiksmus, įvykių audito funkcijos įjungimą ar išjungimą, įvykių audito įrašų trynimą, kūrimą ar keitimą, laiko ir (ar) datos pakeitimus, kitus svarbius saugai įvykius, nurodant RIS naudotojo identifikatorių ir įvykio laiką;

7.3. įvykių audito įrašuose turi būti fiksuojama įvykio data ir tikslus laikas, įvykio rūšis ir (ar) pobūdis, naudotojo ir (ar) RIS administratoriaus, ir (arba) informacinės infrastruktūros įrenginio, susijusio su įvykiu, duomenys bei įvykio rezultatas. Šie duomenys techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti, turi būti saugomi užtikrinant visas prasmingas jų turinio reikšmes ne trumpiau kaip vienus metus kitoje, nei jie įrašomi, sistemoje ir RIS administratoriaus periodiškai analizuojami ir, prireikus ar identifikavus incidento požymius, informuojamas RIS saugos įgaliotinis ar padalinys, vykdantis informacinių sistemų saugos ir kibernetinės saugos politikos įgyvendinimo priežiūrą;

7.4. RIS priežiūros funkcijos atliekamos naudojant tam skirtą RIS administratoriaus identifikatorių, kuriuo naudojantis negalima atlikti kitų RIS naudotojų funkcijų;

7.5. kiekvienas RIS naudotojas unikaliai identifikuojamas pagal jam suteiktą naudotojo vardą ir slaptažodį. Draudžiama suteikti RIS administratoriaus teises RIS naudotojams;

7.6. baigęs darbą ar pasitraukdamas iš darbo vietos, RIS naudotojas privalo imtis priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo RIS, įjungti ekrano užsklandą su slaptažodžiu; dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;

7.7. RIS tarnybinėse stotyse įdiegtos priemonės, įspėjančios RIS administratorių apie laisvos operatyviosios atminties ar laisvos vietos kompiuterių diskuose sumažėjimą iki nustatytos pavojingos ribos, apie ilgą laiką stipriai apkraunamą centrinį procesorių ar kompiuterių tinklo sąsają;

7.8. RIS turi įdiegtas elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

8. Darbo apskaitos priemonės:

8.1. RIS naudotojams suteikiama prieigos teisė atlikti veiksmus tik su jiems priskirta RIS elektronine informacija RIS naudotojų administravimo taisyklėse nustatyta tvarka;

8.2. RIS naudotojų veiksmai su RIS elektronine informacija automatiškai registruojami elektroniniuose žurnaluose.

9. RIS veikla atkuriama vadovaujantis RIS veiklos tęstinumo valdymo ir atstatymo planu.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

10.1. elektroninė informacija į RIS gali būti įvesta, pakeista, atnaujinta tik tam turint teisinį pagrindą ir tik tokius įgaliojimus turinčių RIS naudotojų;

10.2. RIS kaupiama ir apdorojama elektroninė informacija yra skirstoma pagal duomenų savybę, kad duomenys galėtų būti tvarkomi bei naudojami tik RIS naudotojų, turinčių tam teisę;

10.3. teisę keisti priėjimo lygius gali tik RIS administratorius, vadovaudamasis procedūromis, numatytomis RIS naudotojų administravimo taisyklėse bei RIS naudotojų vadovuose;

10.4. kiekviena duomenų pakeitimo operacija yra užfiksuojama duomenų bazėje, taip pat išsaugant ir istorinius duomenis;

10.5. RIS naudotojų tapatybė, jų veiksmai su RIS programine įranga ir elektronine informacija, veiksmų atlikimo laikas atpažįstami programinėmis priemonėmis, automatiškai įrašomi RIS duomenų bazės veiksmų žurnale, apsaugotame nuo nesankcionuoto jame esančių duomenų naudojimo, pakeitimo, iškraipymo, sunaikinimo. Draudžiama veiksmų žurnalo duomenis trinti, keisti, kol nesibaigęs veiksmų žurnalo duomenų saugojimo terminas. RIS duomenų bazės veiksmų žurnalo duomenys prieinami RIS administratoriui ir RIS saugos įgaliotiniui;

10.6. RIS duomenų bazės veiksmų žurnalo įrašai suteikia galimybę nustatyti nesankcionuoto poveikio šaltinį, laiką ar veiksmus RIS programinei įrangai ir elektroninei informacijai;

10.7. RIS naudotojo elektroninės informacijos įrašymo, keitimo, naikinimo veiksmai nurodyti detaliuose RIS naudotojų vadovuose.

11. Prarasta, iškraipyta, sunaikinta RIS elektroninė informacija atkuriama iš RIS atsarginių duomenų kopijų (toliau – Kopijos).

12. Kopijos daromos automatiškai kiekvieną darbo dieną. Kopijos įrašomos į išorines duomenų laikmenas arba saugomos tarnybinėse stotyse, prieinamose RIS administratoriui.

13. Kopijos nuo neteisėto elektroninės informacijos atkūrimo yra apsaugotos naudojant šifravimą. Šifravimo raktai saugomi atskirai nuo Kopijų.

14. Kopijų fizinę apsaugą užtikrina RIS administratorius, jis atsakingas ir už Kopijų darymą bei nukopijuotų duomenų laikmenų perdavimą saugoti.

15. Siekiant užtikrinti RIS elektroninės informacijos atkūrimą, Kopijos privalo būti išsaugomos kiekvieną dieną. Sugedus programinei arba techninei įrangai, RIS elektroninės informacijos atkūrimas turi trukti ne ilgiau kaip 12 valandų. RIS elektroninės informacijos atkūrimo ir Kopijų darymo darbus atlieka RIS administratorius. Veiklos atnaujinimo veiksmų planas numatytas RIS veiklos tęstinumo valdymo plane.

16. Visos elektroninės informacijos atkūrimo procedūros turi būti aprašytos. Už elektroninės informacijos atkūrimo procedūrų aprašymų parengimą atsakingas RIS administratorius.

17. NŠA su susijusių registrų tvarkytojais ir valstybės informacinių sistemų valdytojais sudaro duomenų perdavimo ir gavimo sutartis, kuriose nustatomi duomenų teikimo būdai, terminai, dažnis ir kiti kriterijai. Registrų ir valstybės informacinių sistemų sąveika palaikoma susijusių registrų ir valstybės informacinių sistemų nuostatų ir duomenų perdavimo ir gavimo sutartyje nustatyta tvarka ir sąlygomis automatiniu būdu perduodant, atnaujinant duomenis ar jais keičiantis, gautiems duomenims koduoti naudojant tų registrų suteiktus unikalius objektų identifikavimo kodus.

18. Neteisėto elektroninės informacijos kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

18.1. RIS naudotojai, pastebėję esamus arba galimus saugos dokumentų reikalavimų pažeidimus, kitų RIS naudotojų netinkamus veiksmus, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, nedelsdami praneša apie tai RIS administratoriui ir saugos įgaliotiniui;

18.2. RIS administratorius ir saugos įgaliotinis pagal kompetenciją nedelsdami imasi visų įmanomų prevencinių veiksmų, susijusių su neteisėtu elektroninės informacijos naudojimu;

18.3. saugos įgaliotinis apie Tvarkymo taisyklių 18.1 papunktyje nurodytus pažeidimus praneša NŠA direktoriui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

19. RIS pokyčių valdymo pagrindiniai principai pateikiami Tvarkymo taisyklių priede.

20. Programinė ir techninė įranga keičiama laikantis RIS pokyčių valdymo tvarkos (Tvarkymo taisyklių priedas).

21. Nešiojamųjų kompiuterių naudojimo tvarka:

21.1. nešiojamuosiuose kompiuteriuose turi būti įjungtas visiškas standžiojo disko duomenų šifravimas, naudojamas įjungimo slaptažodis, jei įmanoma, turi būti aktyvuotas BIOS slaptažodis;

21.2. nenaudojami nešiojamieji kompiuteriai turi būti saugomi NŠA saugioje vietoje;

21.3. išnešti iš NŠA patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose. Kelionės metu už nešiojamųjų kompiuterių fizinį saugumą atsakingi jų naudotojai;

21.4. iš perduodamų remontuoti kompiuterių turi būti pašalinta visa su RIS susijusi informacija.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

22. Už saugų RIS elektroninės informacijos tvarkymą atsakingi RIS naudotojai, saugos įgaliotinis, RIS administratorius.

23. Už Tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas saugos įgaliotinis.

24. RIS naudotojai, saugos įgaliotinis, RIS administratorius turi laikytis Tvarkymo taisyklių reikalavimų.

25. Pažeidę Tvarkymo taisykles RIS naudotojai, saugos įgaliotinis, RIS administratorius atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių
priedas

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ KEITIMŲ VALDYMO TVARKA

I SKYRIUS
POKYČIŲ VALDYMO PROCESO PASKIRTIS

1. Pagrindinė pokyčių valdymo proceso paskirtis yra užtikrinti, kad standartizuoti metodai ir procedūros būtų panaudoti efektyviam ir greitam kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų registrų ir valstybės informacinių sistemų (toliau – RIS) pokyčių registravimui, apdorojimui, sprendimų priėmimui, įgyvendinimui užtikrinti ir kartu būtų sumažintas su pokyčiais galimai susijusių incidentų neigiamas poveikis.

2. Pokyčių valdymo procesui keliami šie pagrindiniai uždaviniai:

2.1. sumažinti pokyčių realizavimo kaštus ir riziką;

2.2. užtikrinti pokyčių valdymo proceso integralumą su kitais informacinių technologijų paslaugų valdymo procesais;

2.3. užtikrinti standartizuotą būdą visiems RIS infrastruktūros pokyčiams atlikti ir valdyti;

2.4. apibrėžti pokyčių valdymo procese dalyvaujančių asmenų vaidmenis, jiems deleguojamas atsakomybes.

3. Pokyčių valdymas taikomas RIS techninės, sisteminės ir taikomosios programinės įrangos keitimams, RIS dokumentacijos atnaujinimams.

4. Pokyčių valdymo procesas sąveikauja su incidentų valdymo procesu. Pasitelkiant pokyčių valdymo procesą yra sprendžiami incidentai. Incidentų valdymo procesas įgalina aptikti incidentus, kylančius dėl klaidingai įgyvendintų pokyčių.

II SKYRIUS
POKYČIŲ VALDYMO PROCESO DALYVIAI IR JŲ ATSAKOMYBĖ

5. Pokyčių valdymo proceso dalyviai:

5.1. pokyčio proceso savininkas – RIS valdytojo ar tvarkytojo darbuotojas, užtikrinantis pokyčio proceso veikimą ir tobulinimą, vertinantis pokyčio valdymo proceso dalyvių pateiktas pastabas ir pasiūlymus dėl pokyčio valdymo proceso tobulinimo, atsakantis už technologijas ir įrankius, naudojamus pokyčio valdymo procese, prireikus inicijuojantis pokyčio valdymo proceso pokyčius ir jų įdiegimą, sprendžiantis pokyčio valdymo proceso metu iškilusias iš anksto nenumatytas problemas;

5.2. pokyčio iniciatorius – RIS duomenų valdymo įgaliotinis, saugos įgaliotinis ar administratorius, inicijavęs pokytį. Pokyčio iniciatorius užtikrina reikiamų duomenų, susijusių su inicijuojamu pokyčiu, teikimą pokyčių valdymo proceso dalyviams, vertina pokyčio rezultatų atitiktį planuotiems rezultatams. Pokyčio iniciatorius yra atsakingas už galutinių pokyčio rezultatų vertinimą ir tvirtinimą;

5.3. pokyčio koordinatorius – RIS valdytojo ar tvarkytojo darbuotojas, koordinuojantis ir kontroliuojantis pokyčio įgyvendinimą nuo jo inicijavimo iki pabaigos arba atmetimo. Pokyčio koordinatorius užtikrina pokyčio valdymo proceso dalyvių, trečiosios šalies (paslaugų teikėjų) dalyvavimą, komunikaciją tarp jų, vertina duomenų, susijusių su inicijuojamu pokyčiu, išsamumą ir korektiškumą;

5.4. sprendimą priimantis asmuo – RIS valdytojo ar tvarkytojo darbuotojas, kuris vertina vidutinio sudėtingumo vystymo arba plėtros pokyčių (toliau – vystymo pokytis) tikslingumą, prioritetus, įtaką, pokyčiams įgyvendinti reikalingas priemones, būdus;

5.5. pokyčio kūrėjas – RIS tvarkytojo darbuotojas (-ai) ar trečiosios šalies (paslaugų teikėjo) įgaliotas (-i) asmuo (-ys), įgyvendinantis (-ys) veiklas (kūrimo darbus), kad būtų užtikrintas pokyčio rezultatų pasiekimas;

5.6. pokyčio diegėjas – RIS tvarkytojo darbuotojas (-ai) ar trečiosios šalies (paslaugų teikėjo) įgaliotas (-i) asmuo (-ys), įgyvendinantis (-ys) veiklas (diegimo darbus), kad būtų užtikrintas pokyčio rezultatų pasiekimas.

III SKYRIUS
POKYČIO GYVAVIMO CIKLAS

6. Pokyčio gyvavimo ciklo etapai:

6.1. pokyčio poreikio registravimas;

6.2. pokyčio poreikio įvertinimas;

6.3. pokyčio poreikio patvirtinimas;

6.4. pokyčio įgyvendinimas;
6.5. įgyvendinto pokyčio peržiūra;
6.6. pokyčio poreikio uždarymas.

IV SKYRIUS
POKYČIŲ INICIJAVIMAS

7. Pokyčiai identifikuojami analizuojant RIS veiklos poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai, technologiniai aspektai ir tendencijos, esama RIS būklė (sąranka, pažeidžiamumai, atitiktis teisės aktų ir standartų reikalavimams, pasikartojančios sistemos veikimo klaidos ir pan.). Pagal pokyčio tipą pokyčiai gali būti administraciniai, organizaciniai ar techniniai.

8. Pokyčius inicijuoja pokyčio iniciatorius. RIS tvarkytojai gali teikti pasiūlymus dėl reikalingų pokyčių RIS duomenų valdymo įgaliotiniui.

9. Pokyčių inicijavimo pagrindai:
9.1. infrastruktūros tobulinimas ar jos plėtra;
9.2. RIS reorganizavimas ar modernizavimas;
9.3. elektroninių paslaugų asmenims teikimo tobulinimas ir (ar) plėtra;
9.4. RIS tobulinimas ir (ar) plėtra, atsižvelgiant į RIS naudotojų ir administratorių poreikius;
9.5. RIS rizikos vertinimo metu nustatytos rizikos;
9.6. RIS informacinių technologijų saugos reikalavimų atitikties vertinimo metu nustatyti trūkumai;
9.7. RIS elektroninės informacijos saugos incidentas.

V SKYRIUS
POKYČIŲ VALDYMAS

10. Pokyčio valdymas ir įgyvendinimas organizuojamas atsižvelgiant į pokyčių kategorijas:

10.1. standartinis pokytis – pokytis, kuriam galima taikyti standartines procedūras, nes jam atlikti būtini veiksmai yra žinomi, jie nekelia rizikos kokybiškam RIS paslaugų teikimui arba RIS infrastruktūros veikimui užtikrinti ir nereikalauja papildomų lėšų;

10.2. skubus pokytis – pokytis, skirtas aukščiausio prioriteto sutrikimams arba problemoms šalinti ir reikalauja ypatingos įvertinimo, patvirtinimo ir atlikimo skubos, taip pat avariniai pokyčiai (pvz., veiklos atkūrimas likviduojant elektroninės informacijos saugos incidento, stichinės nelaimės, avarijos ar kitų ekstremaliųjų situacijų padarinius);

10.3. vystymo pokytis – pokytis, kuriuo yra kuriamos arba modernizuojamos RIS paslaugos ir su tuo susiję pokyčio atlikimo veiksmai nėra visiškai aiškūs, o pokyčio atlikimas yra susijęs su tam tikra rizika RIS paslaugoms teikti arba visai RIS infrastruktūrai veikti.

VI SKYRIUS
POKYČIŲ ĮGYVENDINIMAS

11. Pokyčiai, galintys sutrikdyti ar sustabdyti RIS darbą, daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti testuoti skirtoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo RIS darbinės aplinkos. Pokyčiai darbinėje aplinkoje gali būti vykdomi tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių (pvz., veiklos atkūrimas ir kitos avarinės situacijos ir pan.) pokyčių nėra galimybės patikrinti testuoti skirtoje RIS aplinkoje.

12. Nustačius, kad pokyčiams testuoti skirtoje testavimo aplinkoje rezultatas atitinka laukiamus rezultatus, pokyčiai gali būti atliekami darbinėje RIS aplinkoje.

13. Pokyčio koordinatorius turi informuoti RIS naudotojus, susijusius RIS tvarkytojus, kitus suinteresuotus asmenis apie pokyčius, kurių įgyvendinimo metu galimi RIS darbo sutrikimai. Apie pokyčius turi būti informuojama pokyčius įgyvendinančio subjekto interneto svetainėje, RIS taikomosiose programose ar kitomis priemonėmis (pvz., raštu, faksu, elektroniniu paštu ir pan.) ne 5 vėliau kaip prieš 3 (tris) darbo dienas iki planuojamo pokyčio įgyvendinimo pradžios. Šio punkto nuostatų gali būti nesilaikoma, jeigu įgyvendinami skubūs pokyčiai.

14. Įgyvendinus pokytį, pokyčio koordinatorius ir pokyčio iniciatorius turi patikrinti (peržiūrėti) RIS sąranką ir RIS būsenos rodiklius, palyginti ir pagal kompetenciją įvertinti, ar pokytis atitinka planuojamus rezultatus. Sudėtingiems ir specifinių pokyčių rezultatams įvertinti gali būti pasitelkti ir kiti RIS valdytojo, RIS tvarkytojo ar trečiosios šalies (paslaugų teikėjo) kompetentingi specialistai.

VII SKYRIUS
POKYČIŲ DOKUMENTAVIMAS

15. Pokyčio iniciatoriui įsitikinus, kad pokytis atitinka planuotus rezultatus, pokyčio koordinatorius turi atnaujinti RIS sąrankos aprašus ir prireikus inicijuoti kitų, su pokyčiu susijusių, dokumentų atnaujinimus.

16. Jei siekiant įgyvendinti vystymo pokytį turi būti keičiami RIS nuostatai ar kiti RIS veiklą reglamentuojantys teisės aktai, jų pakeitimo projektą nustatyta tvarka rengia pokyčio iniciatorius ar kitas RIS

valdytojo ar tvarkytojo paskirtas asmuo. Vystymo pokyčiai taip pat turi būti dokumentuojami ir RIS techniniuose aprašymuose (specifikacijose).

PATVIRTINTA
Lietuvos Respublikos švietimo, mokslo
ir sporto ministro 2025 m. sausio 16 d.
įsakymu Nr. V-37

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklės (toliau – Administravimo taisyklės) reglamentuoja Švietimo mokslo ir sporto ministerijos kai kurių valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir informacinių sistemų (toliau – RIS) naudotojų ir administratorių teises ir pareigas, RIS naudotojų administravimo principus ir tvarką, jų veiksmų kontrolę.

2. Už Administravimo taisyklių įgyvendinimo organizavimą ir kontrolę atsako RIS saugos įgaliotinis. Už Administravimo taisyklių įgyvendinimą atsako RIS administratorius.

3. RIS naudotojų – įgaliojimų, teisių, pareigų, jų supažindinimo su saugos dokumentais tvarka ir saugaus RIS tvarkomų duomenų teikimo RIS naudotojams kontrolės tvarkos principai paremti RIS duomenų saugumu, stabilumu, operatyvumu.

4. Administravimo taisyklės taikomos visiems RIS naudotojams, RIS administratoriui ir RIS saugos įgaliotiniui.

II SKYRIUS
RIS NAUDOTOJŲ IR ADMINISTRATORIAUS ĮGALIOJIMAI, TEISĖS IR PAREIGOS

5. RIS naudotojai gali naudotis tik tomis RIS dalimis ir posistemėmis bei RIS apdorojamais duomenimis, prie kurių prieigą jiems suteikė RIS administratorius.

6. RIS naudotojų registravimą ir administravimą vykdo RIS administratorius.

7. RIS naudotojų prieigos prie RIS duomenų principai:

7.1. prieiga suteikiama tik prie tų RIS duomenų ir tokia apimtimi, kuri reikalinga RIS naudotojo pareigybės aprašyme nurodytoms funkcijoms atlikti;

7.2. RIS duomenis gali keisti (sukurti, papildyti, taisyti ar panaikinti) tik tokią teisę turintys RIS naudotojai;

7.3. prieiga prie RIS duomenų ir teisė ją keisti suteikiama tik atlikus RIS naudotojo identifikavimą ir patvirtinus jo tapatybę.

8. Prieigos teisių prašymai turi būti registruojami elektroninėmis priemonėmis ar kitu būdu.

9. RIS naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, neteisėtos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai RIS administratoriui arba RIS saugos įgaliotiniui.

10. RIS naudotojai turi teisę reikalauti iš RIS administratoriaus užtikrinti tinkamą jų naudojamo RIS ir jo apdorojamų duomenų apsaugos lygį, gauti informaciją apie taikomas apsaugos priemones ir rekomenduoti papildomas apsaugos priemones.

11. RIS administratorius turi teisę:

11.1. matyti institucijų visus duomenis;

11.2. atlikti duomenų paiešką pagal pasirinktus užklausos kriterijus;

11.3. stebėti RIS funkcionavimą ir pašalinti netikslumus;

11.4. kurti RIS naudotojų prisijungimus.

12. RIS naudotojai turi teisę:

12.1. matyti savo institucijos duomenis;

12.2. tvarkyti savo institucijos duomenis;

12.3. atlikti duomenų paiešką pagal pasirinktus užklausos kriterijus;

12.4. tam tikrais atvejais kurti RIS naudotojų prisijungimus jiems pavaldžių institucijų RIS naudotojams.

13. RIS administratorių, RIS naudotojų veiksmai, duomenų registravimo, duomenų koregavimo veiksmai nurodyti atskirai kiekvieno RIS duomenų saugos nuostatuose ir (arba) vartotojo vadove.

14. RIS administratorių, RIS naudotojų veiksmų registravimas vyksta automatiškai, tam sukurtomis programinės įrangos priemonėmis. Yra fiksuojami visi naudotojų atlikti veiksmai.

15. Už RIS naudotojų supažindinimą su RIS saugos nuostatais, saugaus elektroninės informacijos tvarkymo taisyklėmis, veiklos tęstinumo valdymo planu, Administravimo taisyklėmis atsakingas RIS saugos įgaliotinis. RIS saugos įgaliotinis naujai paskirtus RIS naudotojus pasirašytinai supažindina su RIS saugos dokumentais. RIS naudotojas gali dirbti su RIS elektronine informacija tik pasirašytinai susipažinęs su RIS saugos dokumentais. Jei RIS saugos dokumentuose atsiranda pakeitimų, RIS saugos įgaliotinis su jais supažindina visus RIS naudotojus.

16. RIS saugos įgaliotinis duomenų saugos klausimais ne rečiau kaip kartą per metus RIS administratoriui ir RIS naudotojams elektroniniu ar kitu priimtinu būdu supažindina šiuos asmenis su saugumo politiką reglamentuojančiais teisės aktais, saugaus darbo su duomenimis būdais.

17. RIS tvarkytojo vadovas sudaro galimybes RIS administratoriui, RIS naudotojams dalyvauti RIS saugos įgaliotinio organizuojamuose elektroninės informacijos saugos mokymuose.

18. RIS saugos įgaliotinis nedelsdamas siunčia RIS naudotojams elektroniniu ar kitu priimtinu būdu priimtus naujus elektroninės informacijos saugos teisės aktus ir jų pakeitimus, informuoja apie šiems asmenims organizuojamus kvalifikacijos tobulinimo ir mokymo renginius, priimtiems naujiems RIS naudotojams siunčia atmintines ar kitą aktualią informaciją.

III SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO RIS NAUDOTOJAMS KONTROLĖS TVARKA

19. Visi RIS naudotojai, dirbantys su RIS duomenimis, privalo turėti leidimą dirbti su RIS, t. y. naudotojams turi būti suteikti prisijungimo vardas ir slaptažodis. Unikalus naudotojo vardas ir slaptažodis RIS naudotojui perduodami asmeniškai arba siunčiami elektroniniu paštu užšifruotame dokumente. Nutraukus darbo santykius su RIS naudotoju, atitinkamos įstaigos atsakingas asmuo informuoja el. paštu ir (arba) paprastu paštu apie tai RIS administratorių, kuris panaikina RIS naudotojo prisijungimo vartotojo vardą ir slaptažodį.

20. RIS naudotojui jungiantis prie RIS, jo tapatybė nustatoma pagal unikalų RIS naudotojo prisijungimo vardą, patvirtinamą asmeniniu slaptažodžiu.

21. Unikalus prisijungimo vardas ir pirminis slaptažodis žinomi tik RIS administratoriui ir RIS naudotojui.

22. Suteiktas naudotojo vardas nekeičiamas. Toks pat naudotojo vardas negali būti suteiktas kitam RIS naudotojui.

22.1. slaptažodžiui neturi būti naudojama asmeninio pobūdžio informacija;

22.2. draudžiama slaptažodžius atskleisti tretiesiems asmenims ir naudoti juos pakartotinai, jungiantis prie kitų informacinių sistemų, taikomųjų programų ar interneto svetainių;

22.3. RIS dalys, atliekančios nutolusio prisijungimo autentifikavimą, draudžia automatiškai išsaugoti slaptažodžius;

22.4. slaptažodžiai negali būti saugomi ir perduodami atviru tekstu;

22.5. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius yra 3 kartai. Neteisingai įvedus didžiausią leistiną slaptažodžių skaičių, RIS turi užsirakinti ir neleisti RIS naudotojui identifikuotis. Atblokuoti RIS naudotojo prisijungimą gali tik RIS administratorius, kuris sukūrė pirminį prisijungimą.

23. Papildomi reikalavimai RIS naudotojų slaptažodžiams:

23.1. gavęs RIS administratoriaus suteiktą vardą ir slaptažodį, turi prisijungti prie RIS, nedelsdamas slaptažodį pakeisti ir jį įsiminti;

23.2. privalo keisti slaptažodį ne rečiau kaip kartą per 3 mėnesius;

23.3. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai, kurie negali kartotis;

23.4. keisdamas slaptažodį, turi bent kartą slaptažodį pakartoti;

23.5. neturi teisės palikti užrašyto slaptažodžio matomoje vietoje;

23.6. pamiršęs slaptažodį, privalo kreiptis į RIS administratorių, kuris suteikė prisijungimo vardą ir pirminį slaptažodį;

23.7. įtaręs, kad tretieji asmenys žino jo slaptažodį, nedelsdamas privalo slaptažodį pakeisti.

24. Naujai paskirtam RIS naudotojui RIS administratorius suteikia naują prisijungimo vardą ir pirminį slaptažodį.

25. RIS administratorius nedelsdamas blokuoja netekusio teisės dirbti su RIS duomenimis RIS naudotojo prisijungimo vardą ir slaptažodį.

26. Nuotoliniam prisijungimui prie RIS išoriniams naudotojams papildomi reikalavimai nekeliami. Nuotolinis prisijungimas galimas tik saugiu HTTP protokolu. Priklausomai nuo informacijos pateikimo į RIS būdo, nuotolinis prisijungimas papildomai gali būti kontroliuojamas pagal prie RIS besijungiančio kompiuterio IP adresą.

PATVIRTINTA
Lietuvos Respublikos švietimo, mokslo
ir sporto ministro 2025 m. sausio 16 d.
įsakymu Nr. V-37

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Valdymo planas) reglamentuoja Švietimo mokslo ir sporto ministerijos kai kurių valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir informacinių sistemų (toliau – RIS) veiklos tęstinumo valdymą, taip pat Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos ir Nacionalinės švietimo agentūros (toliau – NŠA) darbuotojų funkcijas, įgaliojimus ir veiksmus, atkuriant RIS veiklą, įvykus elektroninės informacijos saugos incidentui.

2. Valdymo plano tikslas – nustatyti RIS sistemų administratoriaus, informacinių sistemų saugos įgaliotinio, informacinių sistemų naudotojų ir kitų asmenų veiksmus, esant elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus informacinės sistemos duomenims, techninės, programinės įrangos funkcionavimui.

3. Valdymo planas įsigalioja įvykus elektroninės informacijos saugos incidentui, jo vykdymas yra privalomas elektroninės informacijos saugos incidentų atveju, kurių metu gali kilti pavojus RIS duomenims, RIS techninės, programinės įrangos funkcionavimui. Veiksmai, kurie turi būti atliekami įvykus saugos incidentui, yra nurodyti RIS veiklos tęstinumo valdymo detaliajame plane (Valdymo plano 1 priedas).

4. Valdymo planas privalomas RIS valdytojui, RIS tvarkytojams, visiems RIS naudotojams, RIS administratoriui bei RIS saugos įgaliotiniui.

5. Atsakingų asmenų veiksmai ir įgaliojimai įvykus incidentui:

5.1. RIS saugos įgaliotinis:

5.1.1. koordinuoja elektroninės informacijos saugos incidentų, įvykusių RIS, tyrimą;

5.1.2. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

5.2. RIS naudotojai vykdo Veiklos tęstinumo valdymo grupės nurodymus;

5.3. RIS administratorius vykdo šiame Valdymo plane ir prieduose įvardytas ir jam Veiklos tęstinumo valdymo grupės pavestas užduotis.

6. RIS veikla laikoma atkurta, kai RIS naudotojai, naudodamiesi RIS, vėl gali atlikti savo funkcijas.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

7. Veiklos tęstinumo valdymo grupę sudaro: grupės vadovas, grupės vadovo pavaduotojas, grupės nariai. Veiklos tęstinumo valdymo grupės sudėtis tvirtinama atskiru NŠA direktoriaus įsakymu. RIS saugos įgaliotinis skiriamas Veiklos tęstinumo valdymo grupės nariu.

8. Veiklos tęstinumo valdymo grupės funkcijos:

8.1. analizuoti elektroninės informacijos saugos incidentus ir priimti sprendimus RIS veiklos tęstinumo valdymo klausimais;

8.2. bendrauti su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

8.3. bendrauti su teisėsaugos ir kitomis institucijomis, atsakingomis už nacionalinį elektroninių ryšių tinklų ir informacijos saugumą;

8.4. kontroliuoti finansinių ir kitų išteklių, reikalingų RIS veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, naudojimą;

8.5. užtikrinti elektroninės informacijos fizinę saugą įvykus saugos incidentui;

8.6. vykdyti RIS veiklos atkūrimo priežiūrą ir koordinuoti veiklos atkūrimo veiksmus;

8.7. vykdyti kitas Veiklos tęstinumo valdymo grupei pavestas funkcijas.

9. Veiklos atkūrimo grupę sudaro: grupės vadovas, grupės vadovo pavaduotojas, grupės nariai. Veiklos atkūrimo grupės sudėtis tvirtinama atskiru NŠA direktoriaus įsakymu. RIS saugos įgaliotinis ir RIS administratorius skiriami Veiklos atkūrimo grupės nariais.

10. Veiklos atkūrimo grupės funkcijos:

10.1. organizuoti RIS tarnybinių stočių veikimo atkūrimą;

10.2. organizuoti kompiuterių tinklo veikimo atkūrimą;

10.3. organizuoti RIS elektroninės informacijos atkūrimą;
10.4. organizuoti taikomųjų programų tinkamo veikimo atkūrimą;
10.5. organizuoti darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;
10.6. vykdyti kitas veiklos atkūrimo grupei pavestas funkcijas.
11. RIS veikla atkuriama pagal RIS veiklos tęstinumo valdymo detalųjį planą.
12. Veiklos tęstinumo valdymo ir Veiklos atkūrimo grupių nariai turi reaguoti ir valdyti saugos incidentus, vadovaudamiesi Valdymo plano 1 priede pateiktomis instrukcijomis.
13. Elektroninės informacijos saugos incidentai registruojami RIS elektroninės informacijos saugos incidentų registravimo žurnale (Valdymo plano 2 priedas), už kurio pildymą atsakingas RIS administratorius.
14. Saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka.
15. Kad būtų užtikrintas patikimas RIS veikimas, įvykus saugos incidentui, naudojama RIS rezervinė techninė įranga, kuri turi būti laikoma atsarginėje patalpoje, esančioje kitu adresu nei pagrindinė patalpa, kurioje laikoma pagrindinė RIS techninė įranga.
16. Atsarginės patalpos, naudojamos RIS veiklai atkurti įvykus elektroninės informacijos saugos incidentui, turi tenkinti pagrindinėms patalpoms keliamus reikalavimus.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

17. NŠA turi būti parengti ir saugomi šie dokumentai:
17.1. RIS funkcionuoti būtinos informacinių technologijų įrangos parametrų sąrašas (šiame dokumente turi būti numatyti už šios įrangos priežiūrą atsakingi asmenys, jų kompetencijos ir žinių reikalavimai);
17.2. RIS minimalaus funkcionalumo informacinių technologijų įrangos specifikacija (šiame dokumente turi būti nurodyta NŠA poreikius atitinkanti informacinių technologijų įranga RIS veiklai užtikrinti, įvykus elektroninės informacijos saugos incidentui);
17.3. pastato, kuriame yra RIS įranga, patalpų brėžiniai (šiame dokumente turi būti nurodyti kiekvieno pastato aukšto patalpų brėžiniai ir juose pažymėtos tarnybinės stotys, kompiuterių tinklo ir telefonų tinklo mazgai, laidų vedimo tarp pastato aukštų vietos, elektros įvedimo pastate vietos);
17.4. NŠA kompiuterių tinklo fizinio ir loginio sujungimo schemos;
17.5. RIS elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašas (šiame dokumente turi būti nurodyta atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos);
17.6. RIS programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo tvarka (šiame dokumente turi būti nurodyta saugojimo vieta ir laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos);
17.7. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašai, kuriuose nurodyta informacija apie kiekvieną grupės narį (pareigos, vardas, pavardė, mobiliojo bei namų telefonų numeriai, el. pašto adresas, gyvenamosios vietos adresas).

IV SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

18. Valdymo plano veiksmingumas yra išbandomas ne rečiau kaip kartą per metus.
19. Valdymo plano veiksmingumo bandymo metu Veiklos tęstinumo valdymo grupė išanalizuoja sumodeliuotą elektroninės informacijos saugos incidentą, numato galimus jo valdymo būdus ir sprendimus.
20. Išbandžius Valdymo plano veiksmingumą, RIS saugos įgaliotinis parengia Valdymo plano veiksmingumo išbandymo ataskaitą (Valdymo plano 3 priedas). Parengtą ataskaitą saugos įgaliotinis pateikia RIS valdytojui.

Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano
1 priedas

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO DETALUSIS PLANAS

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai	Terminai
1. Oro sąlygos (smarkus lietus, labai smarki audra, viesulas, škvalas, kruša, žemės drebėjimas, smarkus speigas)	1.1. Saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Saugos incidento metu padarytos žalos įvertinimas	RIS saugos įgaliotinis, RIS administratorius	2 d.
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	RIS saugos įgaliotinis, RIS administratorius	1 d.
		1.1.3. Priemonių plano įgyvendinimas	RIS saugos įgaliotinis, RIS administratorius	Iki elektroninės informacijos saugos incidento pašalinimo
	1.2. Darbuotojų saugos incidento pasekmėms likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų instruktavimas, veiksmų koordinavimas	RIS saugos įgaliotinis, RIS administratorius	Nuolat
	1.3. Oro prognozės sekimas	1.3.1. Atsakingų darbuotojų instruktavimas	RIS saugos įgaliotinis, RIS administratorius	Nuolat
	1.4. Rekomendacijų teikimas darbuotojams, dirbantiems pavojaus vietoje	1.4.1. Saugos incidento pasekmes likviduojančių darbuotojų instruktavimas	RIS saugos įgaliotinis, RIS administratorius	Nuolat
		1.4.2. Darbuotojų informavimas apie elgseną pavojaus vietoje	RIS saugos įgaliotinis	Nuolat
		1.4.3. Pirmosios pagalbos suteikimo organizavimas nukentėjusiems darbuotojams	RIS saugos įgaliotinis	Nuolat
	1.5. Pavojaus vietų ženklinimas	1.5.1. Darbuotojų informavimas 1.5.2. Žalą likviduojančių darbuotojų instruktavimas	RIS saugos įgaliotinis, RIS administratorius	Nuolat
2. Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei gauta rekomendacija	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
		2.1.2. Darbuotojų evakavimo organizavimas, jei yra rekomenduojama tai padaryti	RIS saugos įgaliotinis	Nedelsiant
	2.2. Darbuotojų evakavimas (pagal priešgaisrinės gelbėjimo tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	RIS saugos įgaliotinis	Nedelsiant

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai	Terminai
	2.3. Darbas pavojaus zonoje	2.3.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	RIS saugos įgaliotinis	Nedelsiant
	2.4. Komunikacijų, sukeliančių pavojų, išjungimas. Gaisro gesinimas ankstyvoje stadijoje	2.4.1. Priešgaisrinės gelbėjimo tarnybos nurodymų vykdymas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
3. Patalpų užgrobimas	3.1.Teisėsaugos institucijų informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos institucijos rekomendacijos	RIS saugos įgaliotinis	Nedelsiant
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei gauta rekomendacija	RIS saugos įgaliotinis	Nedelsiant
	3.2. Darbuotojų evakavimas, jei yra rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	RIS saugos įgaliotinis	Nedelsiant
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos institucijos nurodymų vykdymas	RIS saugos įgaliotinis	Nedelsiant
	3.4. Teisėsaugos institucijos nurodymų vykdymas, jei yra rekomendacijų	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	RIS saugos įgaliotinis	Nedelsiant
	3.5. Veiksmai išlaisvinus užgrobtas patalpas	3.5.1. Padarytos žalos įvertinimas	RIS saugos įgaliotinis, RIS administratorius	1 d.
		3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	RIS saugos įgaliotinis, RIS administratorius	1 d.
		3.5.3. Žalą likviduojančių darbuotojų instruktavimas	RIS administratorius	Nuolat
4. Patalpai padaryta žala arba patalpos praradimas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.1. Suinteresuotos tarnybos rekomendacijų dėl galimybę dirbti pavojaus zonoje gavimas	RIS saugos įgaliotinis	Nedelsiant
		4.1.2. Darbuotojų informavimas apie rekomendacijas	RIS saugos įgaliotinis	Nuolat
	4.2. RIS įrangos perkėlimas į atsargines patalpas	4.2.1. Darbuotojų informavimas apie darbą patalpose	RIS saugos įgaliotinis	1 d.
5. Energijos tiekimo sutrikimai	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas, tarnybinių stočių, kitos techninės įrangos energijos maitinimo išjungimas	5.1.1 Sutrikimų šalinimo organizavimas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
	5.2. Kreipimasis į energijos tiekimo įmonę dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	5.2.1. Rekomendacijų iš energijos tiekimo įmonės gavimas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
	5.3. Sutrikimų pašalinimas	5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
		5.3.2. Padarytos žalos įvertinimas	RIS saugos įgaliotinis, RIS administratorius	2 d.
		5.3.3. Žalą likviduojančių darbuotojų instruktavimas	RIS saugos įgaliotinis	Nedelsiant

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai	Terminai
6. Vandentiekio ir šildymo sistemos sutrikimai	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	6.1.1. Vandentiekio ar šildymo paslaugų teikėjų paklausimas dėl leidimo dirbti ir rekomendacijų gavimas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
		6.1.2. Darbuotojų informavimas apie rekomendacijas	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
	6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.2.1. Padarytos žalos įvertinimas, sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas	RIS saugos įgaliotinis, RIS administratorius	2 d.
		6.2.2. Žalą likviduojančių darbuotojų instruktavimas	RIS saugos įgaliotinis	Nuolat
7. Ryšio sutrikimai	7.1. Ryšio sutrikimo priežasčių nustatymas	7.1.1. Kreiptis į ryšio paslaugos teikėją	RIS saugos įgaliotinis, RIS administratorius	Nedelsiant
	7.2. Ryšio paslaugų teikėjo informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.2.1. Nustatyti ir įgyvendinti priemones, apsaugančias nuo ryšio sutrikimų pasikartojimo	RIS saugos įgaliotinis, RIS administratorius	2 d.
	7.3. Sutrikimo pašalinimas	7.3.1. Paslaugos teikėjo nurodymų vykdymas	RIS administratorius	Nedelsiant
8. Tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas	8.1. Pranešti teisėsaugos institucijai, draudimo bendrovei apie įvykį	8.1.1. Darbuotojų saugos incidento pasekmėms likviduoti paskyrimas, instruktavimas, jų veiksmų nustatymas	RIS administratorius, RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	Nedelsiant
	8.2. Saugos incidento pasekmių šalinimas	8.2.1. Kreiptis į įrangos tiekėjus dėl įrangos remonto ar naujos įrangos įsigijimo	RIS administratorius	Nedelsiant
		8.2.2. Įsigytos įrangos diegimas	RIS administratorius	Nedelsiant
9. Programinės įrangos sugadinimas, praradimas	9.1. Saugos incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	9.1.1. Saugos incidento metu padarytos žalos įvertinimas	RIS administratorius, RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	2 d.
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	RIS administratorius, RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	1 d.

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Atsakingi pasekmės likvidavimo vykdytojai	Terminai
	9.2. Darbuotojų saugos incidento pasekmei likviduoti paskyrimas, žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų instruktavimas	RIS administratorius, RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	Nuolat
		9.2.2. Kreipimasis į teisėsaugos institucijas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	RIS administratorius, RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	Nedelsiant
10. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas	10.1. Saugos incidento pasekmių įvertinimas	10.1. Prarastų, iškraipytų ar sunaikintų RIS duomenų ir dokumentų atkūrimas	RIS administratorius	1 d.
		10.2. Prarastų, iškraipytų ar sunaikintų RIS duomenų ir dokumentų atkūrimo kontrolė	RIS saugos įgaliotinis, RIS tvarkytojo darbuotojas, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	Nuolat

Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano
2 priedas

(Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS IR KIBERNETINIŲ INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20__m. _____d.

Eil Nr.	Elektroninės informacijos saugos incidentas					
	RIS tvarkytojo pavadinimas	Požymio kodas	Elektroninės informacijos saugos incidento aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Saugos incidentą pašalino (vardas, pavardė)

Elektroninės informacijos saugos incidento požymiai:

1 – gaisras; 2 – elektros energijos tiekimo sutrikimai; 3 – įsilaužimas į vidinį kompiuterių tinklą; 4 – vandentiekio ir šildymo sistemos sutrikimai; 5 – kondicionavimo sistemos sutrikimas; 6 – ryšio sutrikimai; 7 – tarnybinių stočių vagystė arba sugadinimas; 8 – programinės įrangos sugadinimas ar praradimas; 9 – vagystė iš duomenų bazės ar jos fizinis sunaikinimas; 10 – nešiojamųjų kompiuterių ir juose saugomų duomenų praradimas; 11 – pavojingas (įtartinas) radinys; 12 – kompiuterių virusų, nepageidautinų laiškų (*spam*) atakos; 13 – dokumentų praradimas; 14 – duomenų iš duomenų teikėjų negavimas; 15 – dalinis RIS informacinės sistemos sutrikimas dėl neaiškių priežasčių; 16 – gamtos reiškiniai.

Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano
3 priedas

KAI KURIŲ LIETUVOS RESPUBLIKOS ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO ĮVERTINIMO ATASKAITA

(Grupės susitikimo data)

(Grupės susitikimo data)

Veiklos tęstinumo valdymo plano įvertinime dalyvavo:

1. _____
2. _____
3. _____

Elektroninės informacijos saugos ar kibernetinio incidento (toliau – saugos incidentas) scenarijus:

Saugos incidento poveikis Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomam ir Nacionalinės švietimo agentūros tvarkomam registrui ar valstybės informacinei sistemai:

Saugos incidento valdymo eiga:

Rasti Kai kurių Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos valdomų ir Nacionalinės švietimo agentūros tvarkomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano veiklos tęstinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti veiklos tęstinumo valdymo planą:

_____
(Vardas ir pavardė) (Parašas)

_____
(Vardas ir pavardė) (Parašas)

_____
(Vardas ir pavardė) (Parašas)

_____
(Vardas ir pavardė) (Parašas)

Lietuvos Respublikos švietimo, mokslo
ir sporto ministro 2025 m. sausio 16 d.
įsakymo Nr. V-37
priedas

ŠVIETIMO, MOKSLO IR SPORTO MINISTERIJOS VALDOMŲ IR NACIONALINĖS ŠVIETIMO AGENTŪROS TVARKOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Registro / informacinės sistemos pavadinimas	Registro / informacinės sistemos elektroninės informacijos svarbos kategorija
1.	Mokinių registras	vidutinės svarbos
2.	Neformaliojo švietimo programų registras	vidutinės svarbos
3.	Diplomų, atestatų ir kvalifikacijos pažymėjimų registras	vidutinės svarbos
4.	Studentų registras	vidutinės svarbos
5.	Pedagogų registras	vidutinės svarbos
6.	Išsilavinimo pažymėjimų blankų registras	vidutinės svarbos
7.	Licencijų registras	vidutinės svarbos
8.	Švietimo, mokslo ir sporto institucijų registras	vidutinės svarbos
9.	Studijų, mokymo programų ir kvalifikacijų registras	vidutinės svarbos
10.	Nesimokančių vaikų ir mokyklos nelankančių mokinių informacinė sistema	vidutinės svarbos
11.	Atvira informavimo, konsultavimo ir orientavimo sistema	vidutinės svarbos
12.	Švietimo valdymo informacinė sistema	vidutinės svarbos
13.	Švietimo portalo informacinė sistema	vidutinės svarbos
14.	Nacionalinių egzaminų centralizuota informacinė sistema	vidutinės svarbos
15.	Švietimo įstaigų (išskyrus aukštąsias mokyklas) vadovų informacinė sistema	vidutinės svarbos