ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

ĮSAKYMAS
DĖL ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ, SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ, INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO

2020 m. d. Nr.
Šakiai

Vadovaudamasis Lietuvos Respublikos vietos savivaldos įstatymo 18 straipsnio 1 dalimi, 29 straipsnio 8 dalies 2 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, saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7 ,8 punktais:

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

1.1. Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų administravimo taisykles;

1.2. Šakių rajono savivaldybės administracijos saugaus elektroninės informacijos tvarkymo taisykles;

1.3. Šakių rajono savivaldybės administracijos informacinių sistemų veiklos tęstinumo valdymo planą.

2. P r i p a ž į s t u netekusiu galios Šakių rajono savivaldybės administracijos direktoriaus 2009 m. spalio 15 d. įsakymą Nr. AT-1353 „Dėl Šakių rajono savivaldybės administracijos saugaus elektroninės informacijos tvarkymo taisyklių, informacinių sistemų veiklos tęstinumo valdymo plano, informacinių sistemų naudotojų administravimo taisyklių tvirtinimo“.

Šis įsakymas per vieną mėnesį nuo įsakymo paskelbimo dienos gali būti skundžiamas Lietuvos administracinių ginčų komisijos Kauno apygardos skyriui adresu: Laisvės al. 36, Kaunas, arba Regionų apygardos administracinio teismo Kauno rūmams adresu: A. Mickevičiaus g. 8A, Kaunas.

Administracijos direktorius Dainius Grincevičius

Parengė
Bendrųjų reikalų skyriaus vedėja

Rita Vaičiūnienė
2020-07-30

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2020-08-13 raštu Nr. (4.1 E) 6K-515

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2020 m. d.
įsakymu Nr.

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų administravimo taisyklių (toliau – Administravimo taisyklės) tikslas – nustatyti Šakių rajono savivaldybės administracijos (toliau – Administracija) informacinių sistemų ir registrų (toliau – IS) naudotojų administravimo tvarką.

2. Administravimo taisyklėse vartojamos sąvokos:

2.1. **IS paslaugos** – IS priemonėmis teikiamos elektroninės paslaugos;

2.2. **IS paslaugų gavėjas** – fizinis ar juridinis asmuo, turintis teisę gauti IS paslaugas.

3. Administravimo taisyklėse vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, kituose IS elektroninės informacijos tvarkymą ir saugą reglamentuojančiuose teisės aktuose vartojamas sąvokas.

4. Administravimo taisyklės yra privalomos visiems IS naudotojams ir IS administratoriams.

5. Prieiga prie IS elektroninės informacijos nustatoma vadovaujantis šiais principais:

5.1. prie IS saugomų duomenų ir informacijos apdorojimo priemonių prieigą gali gauti tik tie naudotojai, kuriems tokia teisė buvo suteikta pagal jų vykdomas pareigas, atliekamas funkcijas ir sutartinius įsipareigojimus;

5.2. IS saugomus duomenis gali keisti (sukurti, ištrinti arba papildyti) tik tam teises turintys naudotojai;

5.3. IS naudotojai savo veiksmais neturi sutrikdyti registrų, informacinių sistemų arba informacijos apdorojimo priemonių veiklos, nebent tokia teisė jiems buvo išskirtinai suteikta;

5.4. IS administratoriai yra atsakingi už nenutrūkstamą sistemų veikimą ir sistemų naudojamų techninių resursų priežiūrą;

5.5. IS naudotojų veiksmai yra fiksuojami, taip užtikrinant naudotojų atsakomybę už atliktus veiksmus;

5.6. IS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą IS administratoriaus paskyrą, kuria naudojantis negalima atlikti IS naudotojo funkcijos;

5.7. IS naudotojams negali būti suteikiamos IS administratoriaus teisės;

5.8. kiekvienas IS naudotojas turi būti IS unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip IS naudotojo identifikatorius).

II SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. IS naudotojų ir administratorių įgaliojimai, teisės ir pareigos naudotis suteiktomis prieigomis yra nustatomi IS nuostatuose, IS duomenų saugos nuostatuose, IS saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose IS elektroninių paslaugų teikimą.

7. IS naudotojų įgaliojimai, teisės ir pareigos:

7.1. IS naudotojai turi teisę:

7.1.1. naudotis tik tomis IS funkcijomis ir IS kaupiama elektronine informacija tokia apimtimi, kol ji perduodama tvarkyti į kitas IS, prie kurios prieigą jiems suteikė IS administratorius;

7.1.2. tik pagal jiems priskirtas teises gali tvarkyti (sukurti, redaguoti, papildyti ar panaikinti) IS elektroninę informaciją.

7.2. IS naudotojai privalo:

7.2.1. užtikrinti jų naudojamos IS elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti IS elektroninės informacijos prieinamumo;

7.2.2. saugoti tvarkomų asmens duomenų paslaptį Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka;

7.2.3. naudoti tik tas prieigos prie IS elektroninės informacijos teises, kurios buvo suteiktos.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

8. Už IS naudotojų registravimą, išregistravimą, prieigos prie IS teisių suteikimą ir panaikinimą yra atsakingas IS administratorius. IS naudotojui prieiga prie IS duomenų ir elektroninės informacijos suteikiama tik atsižvelgiant į jo pareigybės aprašyme nustatytas funkcijas ir jam pasirašius Administravimo taisyklių priede pateiktą pasižadėjimą laikytis informacinių sistemų saugos reikalavimų.

9. IS administratorius IS naudotojams suteikia prisijungimo prie IS duomenis (vardą ir laikiną slaptažodį), kuriuos išsiunčia IS naudotojui elektroniniu paštu (laikinas slaptažodis perduodamas atskirai nuo vartotojo vardo).

10. IS naudotojo slaptažodžiui yra keliami šie reikalavimai:

10.1. slaptažodis turi būti iš ne mažesnės kaip 8 simbolių kombinacijos, sudarytos iš raidžių, skaičių ir specialiųjų simbolių;

10.2. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

10.3. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius.

11. IS naudotojas privalo:

11.1. pirmą kartą gavęs IS administratoriaus suteiktą vardą ir slaptažodį prisijungti prie IS bei nedelsdamas pakeisti slaptažodį nauju ir jį įsiminti (draudžiama užrašytus slaptažodžius palikti matomoje vietoje);

11.2. saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;

11.3. nedelsdamas jį pakeisti, jei įtaria, kad tretieji asmenys sužinojo slaptažodį.

12. IS administratorių slaptažodžiams yra keliami šie reikalavimai:

12.1. slaptažodis turi būti iš ne mažesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

12.2. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius.

13. IS naudotojui teisė dirbti su konkrečia Elektronine informacija yra ribojama ar sustabdoma, kai IS naudotojas atostogauja, vyksta IS naudotojo veiklos tyrimas ir pan. IS naudotojui teisė dirbti su konkrečia elektronine informacija turi būti sustabdoma, kai įstatymų nustatytais atvejais IS naudotojas nušalinamas nuo darbo (pareigų). Pasibaigus tarnybos (darbo) santykiams, IS naudotojo teisė naudotis informacine sistema turi būti panaikinta nedelsiant.

14. Jei IS naudotojas perkeliamas į kitas pareigas, jam suteiktos IS naudotojo teisės pakeičiamos atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

15. IS naudotojui teisė naudotis IS panaikinama:

15.1. pasibaigus tarnybos ar darbo santykiams;

15.2. netekus teisės naudotis IS duomenimis.

16. Nuotolinis IS naudotojų prisijungimas prie IS turi būti vykdomas protokolu, skirtu duomenų šifravimui ir leidžiamas tik teisės aktų nustatyta tvarka.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

17. Asmenys, kuriems taikomos Administravimo taisyklės, pažeidę šių taisyklių ir kitų saugos politiką įgyvendinančių dokumentų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

Šakių rajono savivaldybės
administracijos informacinių
sistemų naudotojų administravimo
taisyklių priedas

PASIŽADĖJIMAS
LAIKYTIS ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINŲ SISTEMŲ SAUGOS REIKALAVIMŲ

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

Aš,_____,
(vardas, pavardė)

Vadovaudamasis Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugą reglamentuojančių teisės aktų nuostatomis, tvarkydamas ir / ar naudodamas informacinių sistemų duomenis,

1. **Pasižadu:**

1.1. tvarkyti informacinių sistemų duomenis tik tada ir tik tiek, kiek tai būtina numatytoms funkcijoms atlikti;

1.2. neatskleisti duomenų ir nesuteikti kitokios galimybės bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

1.3. savavališkai nediegti informacinių sistemų taikomosios programinės įrangos pakeitimų ir naujų versijų neturėdamas tam teisės aktų nustatyta tvarka suteiktų teisių;

1.4. neatskleisti ar kitaip nesudaryti sąlygų pasinaudoti kitiems asmenims prisijungimo prie informacinių sistemų vardais, slaptažodžiais;

1.5. nenaudoti informacinių sistemų duomenų kitokiais nei informacinių sistemų nuostatuose, kituose teisės aktuose, duomenų teikimo ar paslaugų teikimo sutartyje nurodytais tikslais;

1.6. nesudaryti sąlygų pasinaudoti informacinių sistemų technine ir programine įranga tokios teisės neturintiems asmenims;

1.7. neatlikti veiksmų, dėl kurių gali būti neteisėtai pakeisti ar sunaikinti informacinių sistemų duomenys;

1.8. neatlikti bet kokių kitų neteisėtų informacinių sistemų tvarkymo veiksmų.

2. Patvirtinu, jog esu įspėtas, kad:

2.1. šis pasižadėjimas galios neterminuotą laiką;

2.2. už šio pasižadėjimo nesilaikymą turėsiu atsakyti pagal galiojančius Lietuvos Respublikos teisės aktus.

_____ _____ _____
(pareigos) (parašas) (vardas, pavardė)

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2020 m. birželio d.
įsakymu Nr.

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šakių rajono savivaldybės administracijos saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, užtikrinančią saugų Šakių rajono savivaldybės administracijos informacinių sistemų techninės, programinės įrangos funkcionavimą, saugų duomenų tvarkymą ir jų teikimą kitoms institucijoms pagal teisės aktų nustatytus reikalavimus.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ bei Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Šios Taisyklės yra privalomos visiems Šakių rajono savivaldybės (toliau – Savivaldybė) administracijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartį, naudojantiems kompiuterinę įrangą darbo užduotims atlikti.

4. Šiose Taisyklėse vartojamos sąvokos:

4.1. **Savivaldybės administracijos informacinės sistemos** (toliau – IS) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Savivaldybės administracijos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Savivaldybės administracijos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Savivaldybės administracijos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija.

4.2. Kitos Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

5. Už IS duomenų saugų tvarkymą atsakingi Naudotojai, Administratorius.

6. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas Saugos įgaliotinis.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. Saugiam elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės.

8. Naudojama legali sisteminė ir taikomoji programinė įranga.

9. Programinės įrangos diegimą atlieka tik Administratoriai ar kiti įgalioti asmenys.

10. Naudojamos antivirusinės programos Naudotojų kompiuteriuose, antivirusinės programos elektroninio pašto tarnybinėje stotyje, programinės ugniasienės Naudotojų kompiuteriuose ir tinklo tarnybinėse stotyse apsaugai nuo virusų, šnipinėjimui skirtos programinės įrangos, nepageidaujamo elektroninio pašto ir pan.

11. Siekiant apsaugoti nuo žalingos programinės įrangos, ne rečiau kaip kartą per mėnesį turi būti atliekamas nuolatinis Naudotojų ir tarnybinių stočių operacinių sistemų atnaujinimas.

12. Antivirusinių programų duomenų bazės turi būti atnaujinamos periodiškai – ne rečiau kaip kartą per dieną, jei atnaujinimą pateikia antivirusinės programos gamintojas.

13. Ne rečiau kaip kartą per metus Administratorius atlieka patikrinimą, siekdamas nustatyti, ar IS naudojama programinė įranga yra saugi. Patikrinimą inicijuoja Saugos įgaliotinis.

14. IS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų naudojant ugniasienę.

15. Už tinklo ugniasienių administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią ugniasienių konfigūraciją atsako Administratorius.

16. Saugiam elektroninės informacijos teikimui ir (ar) gavimui iš kitų valstybės institucijų užtikrinti naudojamas Saugus valstybės duomenų perdavimo tinklas (toliau – SVDPT).

17. Naudotojams kompiuterių operacinėse sistemose turi būti suteikiamos teisės, kurios būtinos tiesioginėms pareigoms vykdyti.

18. Duomenys nuo jų praradimo, iškraipymo, sunaikinimo, neteisėto panaudojimo galimybių apsaugomi techninėmis, organizacinėmis, programinėmis priemonėmis.

19. Fizinė prieiga prie IS tarnybinių stočių suteikiama tik informacinių technologijų darbuotojams.

20. Techninė įranga apsaugoma nuo elektros srovės svyravimų, nuo neteisėtos prieigos prie techninės įrangos, jos sugadinimo ar neteisėto poveikio jai. Naudojami specialūs maitinimo šaltiniai, nenutrūkstamo maitinimo šaltinis su automatine apsauga nuo įtampos svyravimų.

21. Patalpa, kurioje veikia tarnybinės stotys atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra.

22. Tarnybinių stočių patalpoje įrengta oro kondicionavimo sistema.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

23. IS duomenų keitimą, atnaujinimą ir naujų duomenų įvedimą turi teisę atlikti tik autorizuoti Naudotojai, turintys teisę tai atlikti.

24. Naudotojų tapatybė ir veiksmai su IS duomenimis fiksuojami programinėmis priemonėmis. Fiksuojamas tikslus prisijungimo, atsijungimo ir duomenų keitimo laikas, vartotojo vardas.

25. Už IS duomenų atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsako Administratorius.

26. Atsarginės duomenų kopijos daromos periodiškai, bet ne rečiau kaip kartą per mėnesį, o kopijos tarnybinėse stotyse – automatiniu būdu į išorinius informacijos kaupiklius.

27. Prarasti, iškraipyti ar sunaikinti Informacinių sistemų duomenys atkuriami iš atsarginių duomenų kopijų.

28. Duomenų atstatymas iš atsarginių kopijų turi būti periodiškai išbandomas – ne rečiau kaip kartą per metus.

29. Atstatymų išbandymą inicijuoja Saugos įgaliotinis.

30. Duomenų perkėlimo ir teikimo kitoms IS bei duomenų gavimo iš jų tvarka nustatoma atskiromis sutartimis.

31. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką, priklausomai nuo konkretaus atvejo, derina Administratorius.

32. Operacinių sistemų ir taikomosios programinės įrangos keitimai turi būti valdomi: planuojami ir ištestuojami, numatomos atstatomosios procedūros nesėkmingų keitimų atvejams, įvertinamas keitimų poveikis saugumui.

33. Už operacinių sistemų ir taikomosios programinės įrangos keitimų valdymą atsakingas Administratorius.

34. Administratorius, užtikrindamas IS duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacinei sistemai ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų.

35. Naudotojas, įtaręs, kad su IS duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Administratoriui. Administratorius, įtaręs, kad su IS duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Saugos įgaliotiniui. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su IS arba su IS tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras.

36. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

36.1. nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti saugomi ir negali būti palikti be priežiūros viešose vietose;

36.2. visi nešiojamieji kompiuteriai ir kiti mobilieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais, sudėtingumu atitinkančiais naudotojų administravimo taisyklių reikalavimus.

36.3. nešiojamuosiuose kompiuteriuose esantys duomenys turi būti šifruojami.

IV SKYRIUS
REIKALAVIMAI, KELIAMI IS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

37. Administratorius suteikia prieigos prie IS duomenų teisę (peržiūrėti duomenis, atlikti užklausas, vykdyti veiksmus su duomenimis ir kt.) bei fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti.

38. Administratorius, suteikdamas prieigos prie IS duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie IS duomenų sąlygomis.

39. Pasibaigus sutartyje nurodytam laikotarpiui, Administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie IS duomenų teisę ir apie tai jį informuoja.

40. Reikalavimai IS, reikalingoms paslaugų teikėjams ir jų projektavimo, aptarnavimo ir priežiūros teikiamoms paslaugoms funkcionuoti nustatomi šių paslaugų teikimo sutartyse.

41. Paslaugų teikimo sutartyse turi būti iš anksto nustatyta, kad paslaugų teikėjas ar įrangos tiekėjas užtikrina atitiktį kibernetinio saugumo reikalavimams, nustatytiems 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“

42. Paslaugų teikimo sutartyse turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja programinę įrangą naudodamas:

43.1. įgyvendintas elektroninės informacijos saugos priemones nuo sankcionuoto poveikio sistemoms, programinei įrangai ir patalpoms;

43.2. sertifikuotą sisteminę programinę įrangą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Naudotojas privalo kuo greičiau informuoti Saugos įgaliotinį ar Administratorių apie pastebėtus saugumo incidentus: šių Taisyklių reikalavimų pažeidimus, IS veiklos sutrikimus arba neįprastą sistemos veikimą.

45. Naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2020 m. sausio d.
įsakymu Nr.

INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Valdymo planas) parengtas pagal Nacionalinį kibernetinių incidentų valdymo planą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. Valdymo planas vykdomas įvykus elektroninės informacijos saugos incidentui, kuris gali sudaryti neteisėto prisijungimo prie savivaldybės informacinių sistemų (toliau – sistemos arba sistema) galimybę, sutrikdyti ar pakeisti sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

2. Valdymo plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo 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, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo““, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, kituose Lietuvos Respublikos įstatymuose ir teisės aktuose.

3. Kibernetinių incidentų valdymas, tyrimas, šalinimas bei pranešimas apie kibernetinius incidentus yra atliekamas vadovaujantis Nacionaliniame kibernetinių incidentų valdymo plane nurodytomis procedūromis. Informacinių sistemų saugos įgaliotinis ir sistemų administratoriai praneša apie incidentus, rengia incidentų tyrimo ataskaitas bei juos analizuoja. Incidentai vertinami ir priskiriami tam tikrai kategorijai vadovaujantis Nacionalinio kibernetinių incidentų valdymo plano priede nurodytais kriterijais. Valdymo planas privalomas sistemos valdytojui, sistemos tvarkytojams, visiems sistemos naudotojams, sistemos administratoriui bei sistemos saugos įgaliotiniui.

4. Atsakingų asmenų veiksmai ir įgaliojimai įvykus incidentui:

4.1. sistemos saugos įgaliotinis:

4.1.1. koordinuoja elektroninės informacijos saugos incidentų, įvykusių sistemoje, tyrimą;

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

4.2. sistemos naudotojai vykdo Veiklos tęstinumo valdymo grupės nurodymus;

4.3. sistemos administratorius:

4.3.1. dalyvauja atliekant Veiklos plano 11 punkte išvardytas funkcijas;

4.3.2. vykdo kitas šiame dokumente arba prieduose įvardytas ir (arba) jam Veiklos tęstinumo valdymo grupės pavestas užduotis;

4.4. sistemos duomenų įgaliotinis suteikia darbo grupėms informaciją, reikalingą duomenims atkurti, bei rezervines duomenų kopijas.

5. Elektroninės informacijos saugos incidento metu patirti nuostoliai sistemos veiklai atkurti finansuojami valstybės biudžeto, kitų finansavimo šaltinių lėšomis.

6. Veiksmų, kurie būtų atliekami įvykus elektroninės informacijos saugos incidentui, vykdymo eiliškumas ir atsakingi vykdytojai nurodyti Šakių rajono savivaldybės informacinės sistemos veiklos atkūrimo detaliajame plane (1 priedas).

7. Sistemos veikla laikoma atkurta, kai sistemos naudotojai, naudodamiesi sistema, vėl gali atlikti savo funkcijas.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

8. Veiklos tęstinumo valdymo grupės sudėtis:

8.1. grupės vadovas – informacinių sistemų saugos įgaliotinis;

8.2. grupės nariai:

8.2.1. administracijos direktorius;

8.2.2. Bendrųjų reikalų skyriaus vedėjas;

8.2.3. Teisės, personalo ir civilinės metrikacijos skyriaus vedėjas.

9. Veiklos tęstinumo valdymo grupės funkcijos:

9.1. analizuoti elektroninės informacijos saugos incidentus ir priimti sprendimus sistemos veiklos tęstinumo valdymo klausimais;

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

9.3. bendrauti su kitų registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

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

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

9.6. užtikrinti elektroninės informacijos fizinę saugą įvykus saugos incidentui;

9.7. organizuoti darbuotojų, daiktų, įrangos gabenimą;

9.8. vykdyti sistemos veiklos atkūrimo priežiūrą ir koordinuoti veiklos atkūrimo veiksmus;

9.9. vykdyti kitas Veiklos tęstinumo valdymo grupei pavestas funkcijas.

10. Veiklos atkūrimo grupės sudėtis:

10.1. grupės vadovas – informacinių sistemų saugos įgaliotinis;

10.2. grupės nariai:

10.2.1. informacinių sistemų administratorius;

10.2.2. kompiuterinių tinklų administratorius;

10.2.3. sistemos duomenų valdymo įgaliotinis.

11. Veiklos atkūrimo grupės funkcijos:

11.1. organizuoti sistemos tarnybinių stočių veikimo atkūrimą;

11.2. organizuoti kompiuterių tinklo veikimo atkūrimą;

11.3. organizuoti sistemos elektroninės informacijos atkūrimą;

11.4. organizuoti taikomųjų programų tinkamo veikimo atkūrimą;

11.5. organizuoti darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

11.6. vykdyti kitas Veiklos atkūrimo grupei pavestas funkcijas.

12. Sistemos veikla atkuriama pagal Informacinės sistemos veiklos atkūrimo detalųjį planą.

13. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės nariai turi reaguoti ir valdyti saugos incidentus, vadovaudamiesi 1 priede pateiktomis instrukcijomis.

14. Tarpusavyje Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės nariai bendrauja asmeniškai, telefonu arba elektroniniu paštu.

15. Elektroninės informacijos saugos incidentai registruojami sistemos elektroninės informacijos saugos incidentų registravimo žurnale Dokumentų valdymo sistemoje arba popieriniame žurnale, už kurio pildymą atsakingas saugos įgaliotinis.

16. Saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka.

17. Kad būtų užtikrintas patikimas sistemos veikimas įvykus saugos incidentui, naudojama sistemos rezervinė techninė įranga, kuri turi būti laikoma atsarginėje patalpoje, esančioje kitu adresu nei pagrindinė patalpa, kurioje laikoma pagrindinė sistemos techninė įranga.

18. Atsarginės patalpos, naudojamos informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, turi tenkinti pagrindinėms patalpoms keliamus reikalavimus. Atsarginėse patalpose turi būti įrengtos saugos priemonės:

18.1. sistemos tarnybinių stočių patalpos apsaugotos nuo neteisėto asmenų patekimo į jas;

18.2. sistemos tarnybinių stočių patalpoje įrengti gaisro davikliai;

18.3. naudojama įėjimo į patalpas kontrolė;

18.4. patalpose naudojami nenutrūkstančio elektros maitinimo šaltiniai;

18.5. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

19. Parengtų saugomų dokumentų sąrašas:

19.1. Sistemos specifikacijos kopija, kurioje nurodyti sistemos techninės ir programinės įrangos parametrai. Specifikacijos projektą rengė Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka parinktas paslaugų teikėjas. Už sistemos techninės ir programinės įrangos priežiūrą atsakingas sistemos administratorius, kuriam keliami kvalifikaciniai reikalavimai, nurodyti Sistemos duomenų saugos nuostatuose, patvirtintuose savivaldybės administracijos direktoriaus.

Nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, jį pavaduoti gali kitas savivaldybės administracijos direktoriaus paskirtas darbuotojas, kurio kompetencijos lygis informacinių technologijų srityje atitinka sistemos administratoriui keliamų reikalavimų lygį;

19.2. savivaldybės administracijos pastato, kuriame yra tarnybinės stotys, patalpų planai, tarnybinių stočių fizinio ir loginio sujungimo schemos. Už šių dokumentų rengimą atsakingas kompiuterinio tinklo priežiūros paslaugas atliekantis paslaugos teikėjas, administruojantis kompiuterinius tinklus;

19.3. sistemos elektroninės informacijos teikimo, programinės įrangos priežiūros sutarčių kopijos, už kurių rengimą atsakingas kompiuterinio tinklo priežiūros paslaugas atliekantis paslaugos teikėjas;

19.4. sistemos techninės ir programinės įrangos sąrašai, kuriuose nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos. Už sistemos techninės ir programinės įrangos sąrašų rengimą atsakingas sistemos administratorius bei duomenų valdymo įgaliotinis;

19.5. sistemos duomenų rezervinių kopijų kūrimo instrukcija, kurioje nurodyta laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos. Už sistemos duomenų rezervinių kopijų kūrimo instrukcijos parengimą atsakingas sistemos administratorius bei duomenų valdymo įgaliotinis;

19.6. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu. Už šių dokumentų parengimą atsakingas sistemos saugos įgaliotinis.

20. Valdymo plano 19 punkte nurodytų dokumentų kopijas saugo sistemos duomenų valdymo įgaliotinis.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

21. Valdymo plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus.

22. Bandymo metu Veiklos tęstinumo valdymo grupė išanalizuoja galimą (sumodeliuotą) elektroninės informacijos saugos incidentą, numato galimus jo valdymo būdus ir sprendimus.

23. Išbandžius Valdymo plano veiksmingumą, sistemos saugos įgaliotinis turi parengti Valdymo plano veiksmingumo išbandymo ataskaitą. Parengtą ataskaitą (2 priedas) saugos įgaliotinis pateikia sistemos valdytojui.

24. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Informacinės sistemos veiklos tęstinumo
valdymo
plano
1 priedas

INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Įvykis, sukeliantis elektroninės informacijos saugos incidentą	**Pasekmės likvidavimo veiksmai**	**Atsakingi vykdytojai**
1. Patalpų pažeidimas arba praradimas, stichinė nelaimė 1.1. Šakių rajono savivaldybės administracijos patalpose	1.1.1. jeigu būtina, skelbti pavojų ir informuoti Veiklos tęstinumo valdymo grupės vadovą;	Pavojų pastebėjęs darbuotojas
	1.1.2. pranešti specialiosioms tarnyboms;	Veiklos tęstinumo valdymo grupės vadovas
	1.1.3. iškviesti Veiklos tęstinumo valdymo grupės narius į saugią vietą;	
	1.1.4. informuoti sistemos veiklos atkūrimo grupės vadovą;	
	1.1.5. iškviesti sistemos veiklos atkūrimo grupės narius į saugią vietą;	Veiklos atkūrimo grupės vadovas
	1.1.6. vykdyti specialiųjų tarnybų nurodymus;	Visi darbuotojai
	1.1.7. organizuoti darbuotojų evakuaciją, suskaičiuoti evakuotus darbuotojus;	Veiklos tęstinumo valdymo grupė
	1.1.8. informuoti specialiąsias tarnybas apie dingusius darbuotojus;	
	1.1.9. gavus rekomendacijas iš specialiųjų tarnybų, informuoti darbuotojus, kaip elgtis esant susidariusiai situacijai;	
	1.1.10. esant būtinybei, išjungti ir užrakinti visą įrangą;	Veiklos atkūrimo grupė

	1.1.11. įvertinti pažeidimus ir padarytus nuostolius;	
	1.1.12. informuoti darbuotojus apie darbo funkcijų vykdymo aplinkybes;	Veiklos tęstinumo valdymo grupė
	1.1.13. nustatyti, ar buvo prarasta įranga;	Veiklos atkūrimo grupė
	1.1.14. įrangos praradimo atveju informuoti veiklos tęstinumo valdymo grupę;	
	1.1.15. vykdyti teisėsaugos organų ir (arba) draudimo įmonės nurodymus, pateikiant reikiamus duomenis apie įvykį;	Veiklos tęstinumo valdymo grupė
	1.1.16. esant poreikiui perskirstyti, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų atkurtas sistemos veikimas;	
	1.1.17. trūkstant išteklių, kreiptis į sistemos valdytoją dėl papildomų resursų skyrimo;	
	1.1.18. įsigijus įrangą, atkurti sistemos veikimą.	Veiklos atkūrimo grupė
1.2. Paslaugos teikėjo, kurio patalpose yra sistemos programinė įranga, patalpos	1.2.1. nustačius sistemos programinės įrangos pažeidimus arba praradimą, nedelsiant informuoti sistemos tvarkytoją;	Veiklos atkūrimo grupės vadovas
	1.2.2. vadovaujantis paslaugos teikimo sutartyje nustatytais įsipareigojimais, vykdyti sistemos programinės įrangos atkūrimo darbus.	Paslaugos teikėjas
2. Gaisras 2.1. Šakių rajono savivaldybės administracijos patalpose	2.1.1. pastebėjus gaisro židinį, stengtis jį užgesinti kuo greičiau;	Pavojų pastebėjęs darbuotojas
	2.1.2. jeigu būtina, skelbti pavojų ir pranešti priešgaisrinei gelbėjimo tarnybai;	
	2.1.3. informuoti Veiklos tęstinumo valdymo grupės vadovą;	
	2.1.4. iškviesti Veiklos tęstinumo valdymo grupę į saugią vietą;	Veiklos tęstinumo valdymo grupės vadovas
	2.1.5. informuoti veiklos atkūrimo grupės vadovą;	
	2.1.6. iškviesti veiklos atkūrimo grupę;	Veiklos atkūrimo grupės vadovas

	2.1.7. vykdyti specialiųjų tarnybų nurodymus;	Visi darbuotojai
	2.1.8. jeigu būtina, organizuoti darbuotojų evakuaciją, suskaičiuoti evakuotus darbuotojus;	Veiklos tęstinumo valdymo grupė
	2.1.9. informuoti specialiąsias tarnybas apie dingusius darbuotojus;	
	2.1.10. gavus rekomendacijas iš specialiųjų tarnybų, informuoti darbuotojus, kaip elgtis pavojaus zonoje;	
	2.1.11. likvidavus gaisrą įvertinti pažeidimus ir patirtus nuostolius;	Veiklos atkūrimo grupė
	2.1.12. esant poreikiui perskirstyti, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų atkurtas sistemos veikimas;	Veiklos tęstinumo valdymo grupė
	2.1.13. nesant pakankamam rezervui, kreiptis į sistemos valdytoją dėl papildomų resursų skyrimo;	
	2.1.14. įsigijus įrangą, atkurti sistemos veikimą.	Veiklos atkūrimo grupė
2.2. Paslaugos teikėjo, kurio patalpose yra sistemos programinė įranga, patalpos	2.2.1. nustačius sistemos programinės įrangos pažeidimus arba praradimą nedelsiant informuoti sistemos tvarkytoją;	Paslaugos teikėjas
	2.2.2. vadovaujantis paslaugos teikimo sutartyje nustatytais įsipareigojimais vykdyti sistemos programinės įrangos atkūrimo darbus.	Paslaugos teikėjas
3. Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui	3.1. informuoti sistemos valdytoją;	Veiklos tęstinumo valdymo grupė
	3.2. vykdyti sistemos programinės įrangos atkūrimo darbus.	Veiklos atkūrimo grupė
4. Pagrindinių duomenų praradimas pažeidus ar kitaip sugadinus centrinę duomenų saugyklą	4.1. nutraukti paslaugų teikimą sistemos naudotojams, jeigu tai kelia pavojų prarasti duomenis ir kitaip pažeisti Sistemos funkcionalumą;	Veiklos tęstinumo valdymo grupė
	4.2. informuoti sistemos naudotojus, jeigu tai sukelia veiklos sutrikimus;	
	4.3. jeigu sistemos duomenys prarasti ar jie tapo prieinami tam leidimo neturintiems asmenims, pranešti teisėsaugos organams;	

	4.4. vykdyti teisėsaugos organų nurodymus, pateikiant reikiamą informaciją apie įvykį;	
	4.5. atkurti sistemos darbingumą;	Veiklos atkūrimo grupė
	4.6. nustatyti, ar atkurti duomenys yra patikimi;	Veiklos atkūrimo grupė
	4.7. jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinti jas;	
	4.8. atkurti sistemos duomenis iš paskutinės geros atsarginės kopijos;	
	4.9. visiškai atkurti sistemos veiklą ir visas sistemos naudotojų galimybes naudotis sistema.	
5. Sistemos veiklos sutrikdymas dėl kibernetinių atakų	5.1. nutraukti paslaugų teikimą sistemos naudotojams ir informuoti juos apie veiklos sutrikimus;	Veiklos atkūrimo grupė
	5.2. nustatyti trikdžių šaltinį;	
	5.3. pranešti elektroninių ryšių ir informacijos saugumo incidentų tyrimo tarnyboms, suteikiant reikiamą informaciją apie įvykį;	Veiklos tęstinumo valdymo grupė
	5.4. patikrinti, ar neprarasti arba nesugadinti sistemos duomenys;	Veiklos atkūrimo grupė
	5.5. pašalinti trikdžius, atkurti sistemos veikimą.	Veiklos atkūrimo grupė
6. Elektros ir telekomunikacinių ryšių tiekimo sutrikimai	6.1. jeigu yra galimybė, nustatyti elektros ir ryšių paslaugų teikimo sutrikimo priežastis;	Veiklos tęstinumo valdymo grupė
	6.2. kreiptis į paslaugų teikėją dėl sutrikimų pašalinimo;	
	6.3. informuoti darbuotojus ir pateikti rekomendacijas, kaip elgtis esant susidariusiai situacijai;	
	6.4. pašalinus sutrikimą, atnaujinti sistemos veikimą.	Veiklos atkūrimo grupė
7. Vandentiekio ar šildymo sistemos avarija	7.1. kreiptis į specialiąsias tarnybas dėl sutrikimų pašalinimo;	Veiklos tęstinumo valdymo grupė
	7.2. informuoti darbuotojus ir pateikti rekomendacijas, kaip elgtis esant susidariusiai situacijai;	

	7.3. pašalinus sutrikimą, atnaujinti sistemos veikimą.	Veiklos atkūrimo grupė

_____

Informacinės sistemos
veiklos
tęstinumo valdymo plano
2 priedas

INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO ATASKAITA

(Grupės susitikimo data)

Veiklos tęstinumo valdymo plano išbandyme dalyvavo:

1. _____
2. _____
3. _____

Elektroninės informacijos saugos incidento scenarijus:

Elektroninės informacijos saugos incidento valdymo eiga:

Rasti veiklos tęstinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti veiklos tęstinumo valdymo planą:

(vardas, pavardė) (parašas)

(vardas, pavardė) (parašas)

(vardas, pavardė) (parašas)

(vardas, pavardė) (parašas)

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Šakių rajono savivaldybė
Dokumento pavadinimas (antraštė)	Dėl Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų administravimo taisyklių, saugaus elektroninės informacijos tvarkymo taisyklių, informacinių sistemų veiklos tęstinumo valdymo plano patvirtinimo
Dokumento registracijos data ir numeris	2020-08-20 14:54 Nr. AT-699
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Dainius Grincevičius Administracijos direktorius
Parašo sukūrimo data ir laikas	2020-08-20 14:54
Parašo formatas	Trumpalaikio galiojimo (XAdES-T)
Laiko žymoje nurodytas laikas	2020-08-20 14:54
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-A
Sertifikato galiojimo laikas	2018-02-05 10:41 - 2021-02-04 10:41
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	4
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	informacinių sistemų naudotojų administravimo taisyklės.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	pasizadejimas.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	saugaus elektronines informacijos tvarkymo taisykles.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	veiklos testinumo planas.docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DekaDoc v.20200814.3
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2020-08-20 15:25 nuorašą suformavo Irena Bacevičienė
Paieškos nuoroda	-
Papildomi metaduomenys	-