ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

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

2024 m. d. Nr.
Šakiai

Vadovaudamasis Lietuvos Respublikos vietos savivaldos įstatymo 34 straipsnio 6 dalies 2 punktu, Lietuvos Respublikos informacinių išteklių valdymo įstatymu, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 4 punktu:

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

1.1. Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatus;

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

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

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

2. P a v e d u Šakių rajono savivaldybės administracijos Bendrųjų reikalų skyriaus vyresniajai sekretorei Irenai Bacevičienei Dokumentų valdymo sistemos „Kontora“ priemonėmis su įsakymu supažindinti Šakių rajono savivaldybės administracijos darbuotojus (skyrių, seniūnijų, į skyriaus sudėtį neįeinančius).

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

3.1. Šakių rajono savivaldybės administracijos direktoriaus 2020 m. rugpjūčio 20 d. įsakymą Nr. AT-698 „Dėl Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais.

3.2. Šakių rajono savivaldybės administracijos direktoriaus 2020 m. rugpjūčio 20 d. įsakymą Nr. AT-699 „Dėl Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų

administravimo taisyklių, saugaus elektroninės informacijos tvarkymo taisyklių, informacinių sistemų veiklos tęstinumo valdymo plano patvirtinimo“ su visais pakeitimais ir papildymais.

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 administracinio teismo Kauno rūmams adresu: A. Mickevičiaus g. 8A, Kaunas.

Administracijos direktorius Vytautas Ižganaitis

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2024-12-23 raštu Nr. (4.1 E) 6K-859

Parengė
Bendrųjų reikalų skyriaus vedėja

Rita Vaičiūnienė
2024-12-

PATVIRTINTA
Šakių rajono savivaldybės administracijos
direktoriaus
2024 m. gruodžio d. įsakymu Nr.

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šakių rajono savivaldybės administracijos (toliau − Savivaldybės administracija) valdomų informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Savivaldybės administracijos valdomų bei tvarkomų informacinių sistemų (toliau – informacinės sistemos) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. Saugos nuostatų reikalavimai taikomi tvarkant informacines sistemas, nurodytas Savivaldybės administracijos informacinių sistemų sąraše (Saugos nuostatų priedas).

3. Elektroninės informacijos saugos politika įgyvendinama pagal Savivaldybės administracijos direktoriaus tvirtinamus informacinių sistemų saugos politiką įgyvendinančius dokumentus – saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau – saugos politiką įgyvendinantys dokumentai).

4. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Bendrųjų saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), vartojamas sąvokas, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai) .

5. Informacinių sistemų elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti Informacinių sistemų elektroninę informaciją;

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

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

5.4. užtikrinti informacinėse sistemose tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

6. Informacinių sistemų elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. elektroninės informacijos tvarkymo bei jos naudojimo kontrolė;

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

6.3. informacinėse sistemose tvarkomų asmens duomenų apsauga;

6.4. informacinių sistemų veikos tęstinumo užtikrinimas.

7. Informacinių sistemų elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

8. Saugos nuostatų reikalavimai taikomi:

8.1. informacinių sistemų valdytojui ir tvarkytojui, Šakių rajono savivaldybės administracijai, Bažnyčios g. 4, Šakiai;

8.2. Savivaldybės administracijos informacijos saugos įgaliotiniui;

8.3. Savivaldybės administracijos administratoriams;

8.4. Savivaldybės administracijos informacinių sistemų naudotojams;

8.5. paslaugų, susijusių su informacinėmis sistemomis, teikėjams.

9. Už elektroninės informacijos saugą pagal kompetenciją atsako informacinių sistemų valdytojas ir tvarkytojas.

10. Informacinių sistemų valdytojas atsako už informacinių sistemų elektroninės informacijos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą, elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo duomenų gavėjams teisėtumą.

11. Informacinių sistemų naudotojai, tvarkantys duomenis, informaciją, dokumentus ir (arba) jų kopijas, privalo įsipareigoti saugoti duomenų ir informacijos paslaptį *(Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų administravimo taisyklių priedas)*. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymu susijusią veiklą.

12. Paslaugų, susijusių su informacinėmis sistemomis, teikėjai, *pasirašydami paslaugų teikimo sutartį, privalo suderinti ir pasirašyti konfidencialumo pasižadėjimo formą, taip* įsipareigojant saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

13. Informacinių sistemų valdytojas atlieka informacinių sistemų nuostatuose nustatytas funkcijas, o taip pat:

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

13.2. prižiūri ir kontroliuoja, kad informacinės sistemos būtų tvarkomos vadovaujantis informacinių sistemų nuostatais, Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

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

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

13.5. priima sprendimus dėl informacinių sistemų elektroninės informacijos saugos priemonių finansavimo;

13.6. skiria saugos įgaliotinį ir administratorius;

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

14. Informacinių sistemų tvarkytojas atlieka informacinių sistemų nuostatuose nustatytas funkcijas, o taip pat:

14.1. užtikrina elektroninės informacijos, esančios informacinių sistemų duomenų bazėse, saugą;

14.2. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

14.3. užtikrina tinkamą Saugos nuostatų, informacinių sistemų saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

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

14.5. planuoja ir įgyvendina priemones, mažinančias duomenų atskleidimo ir praradimo riziką bei užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

14.6. užtikrina, kad informacinės sistemos veiktų nepertraukiamai;

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

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

15. Savivaldybės administracijos saugos įgaliotinis:

15.1. supažindina informacinių sistemų naudotojus su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, atsakomybe už saugos dokumentų nuostatų pažeidimus;

15.2. rengia saugos dokumentų projektus;

15.3. koordinuoja ir prižiūri informacinių sistemų elektroninės informacijos saugos politikos įgyvendinimą;

15.4. koordinuoja informacinių sistemų saugos incidentų tyrimą;

15.5. teikia pasiūlymus Savivaldybės administracijos direktoriui dėl:

15.5.1. informacinių sistemų informacinių technologijų saugos atitikties vertinimo atlikimo;

15.5.2. administratoriaus paskyrimo;

15.6. teikia pasiūlymus informacinių sistemų valdytojui dėl Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

15.7. teikia administratoriams, informacinių sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

15.8. ne rečiau kaip kartą per kalendorinius metus organizuoja administratorių, naudotojų saugos mokymus (surengdamas saugos tematikos mokymus, organizuodamas mokymo paslaugų įsigijimą ar kitais būdais), reguliariai įvairiais būdais informuoja naudotojus apie elektroninės informacijos saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir pan.).

15.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

16. Saugos įgaliotinis negali atlikti administratorių funkcijų.

17. Savivaldybės administracijos direktoriaus įsakymu paskirti administratoriai atlieka funkcijas, susijusias su informacinių sistemų naudotojų administravimu, informacinės sistemos komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais), šių informacinių sistemų komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus ir jų valdymu, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių komponentų būklę.

18. Savivaldybės administracijos direktoriaus įsakymu paskirti administratoriai:

18.1. prižiūri informacinių sistemų ir tinklų infrastruktūrą, užtikrina jų veikimą ir elektroninės informacijos saugą;

18.2. atlieka informacinių sistemų naudotojų administravimo funkcijas (informacinių sistemų naudotojų registravimas ir išregistravimas, prieigos teisių suteikimas ir panaikinimas, informacinių sistemų naudotojų duomenų tvarkymas, klasifikatorių tvarkymas, registracijos žurnalų įrašų analizė ir kt.);

18.3. diegia, konfigūruoja ir prižiūri techninę ir programinę įrangą;

18.4. administruoja ugniasienes, maršrutizatorius, komutatorius;

18.5. užtikrina kompiuterių tinklų saugumą (nustato pažeidžiamas vietas);

18.6. užtikrina tarnybinių stočių veikimą (diegia ir konfigūruoja tarnybinių stočių programinę įrangą, atnaujinimus), saugą;

18.7. užtikrina duomenų bazių veikimą, tvarko duomenų bazių programinę įrangą;

18.8. diegia duomenų bazių programinės įrangos atnaujinimus, kuria ir administruoja duomenų bazių naudotojų registracijos į duomenų bazes duomenis;

18.9. kuria ir atkuria atsargines elektroninės informacijos kopijas;

18.10. pagal kompetenciją reaguoja į saugos incidentus ir juos valdo, atlieka įsilaužimų į informacines sistemas aptikimo funkcijas;

18.11. dalyvauja atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų atitikties saugos reikalavimams vertinimą.

19. Savivaldybės administracijos direktoriaus įsakymu paskirti administratoriai privalo vykdyti visus Savivaldybės administracijos saugos įgaliotinio nurodymus ir pavedimus dėl informacinių sistemų elektroninės informacijos saugos užtikrinimo, pagal kompetenciją reaguoti į saugos incidentus, juos valdyti ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių komponentų būklę.

20. Teisės aktai, kuriais vadovaujantis tvarkoma informacinių sistemų elektroninė informacija ir užtikrinama jos sauga:

20.1. Lietuvos Respublikos informacinių išteklių valdymo įstatymas;

20.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1);

20.5. Bendrųjų saugos reikalavimų aprašas;

20.6. Kibernetinio saugumo reikalavimų aprašas;

20.7. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techniniai reikalavimai);

20.8. Informacinių sistemų nuostatai;

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

20.10. Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“;

20.11. Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“ (toliau – Metodika);

20.12. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. Informacinėse sistemose tvarkomos elektroninės informacijos svarbos rūšis, informacinių sistemų rūšys bei priskyrimo tam tikrai rūšiai kriterijai nurodyti Saugos nuostatų priede.

22. Informacinių sistemų saugos priemonės parenkamos įvertinus galimus rizikos veiksnius elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui.

23. Pagrindinės informacinių sistemų rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet ne vėliau nei iki spalio 30 dienos, o prireikus ir neeilinio rizikos įvertinimo ataskaitą iki informacinių sistemų valdytojos nurodytos datos rengia saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausieji yra šie:

23.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

23.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 84 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano duomenis bei jų kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai (toliau – ARSIS) Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro, nustatyta tvarka.

25. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis informacinių sistemų elektroninės informacijos saugos priemonėmis, kurios pasirenkamos atsižvelgiant į informacinių sistemų valdytojo skiriamus išteklius, vadovaujantis šiais principais:

25.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

25.2. elektroninės informacijos saugos priemonės diegimo kainos turi atitikti saugomos elektroninės informacijos vertę;

25.3. esant galimybei, turi būti įdiegtos prevencinės korekcinės elektroninės informacijos saugos priemonės.

26. Informacinių sistemų valdytojas, atsižvelgdamas į informacinių sistemų rizikos įvertinimo ataskaitą, prireikus tvirtina Rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

27. Siekiant užtikrinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka, kasmet organizuojamas informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimas.

28. Informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir geroja praktika.

29. Atlikus informacinių sistemų informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytojas.

30. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano duomenis ir jų kopijas informacinių sistemų valdytoja arba jos įgaliotas informacinių sistemų tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro, nustatyta tvarka.

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

32. Programinės įrangos, skirtos informacines sistemas apsaugoti nuo kenksmingosios programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

32.1. Informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą, kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

32.2. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

33. Programinės įrangos, įdiegtos informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

33.1. informacinių sistemų darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į leistinos programinės įrangos sąrašą.

33.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

33.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka administratoriai;

34. Informacinėse sistemose turi būti naudojamos tik tarnybinės išorinės duomenų laikmenos (USB, CD/DVD ir kt.) bei kiti tarnybiniai įrenginiai, kurie yra išduoti tarnybinėms funkcijoms vykdyti.

35. Informacinių sistemų kompiuterizuotose darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti išorinių duomenų laikmenų (USB, CD/DVD ir kt.) naudojimą.

36. Informacinių sistemų programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

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

37.1. Kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

37.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos;

37.3. turi būti naudojamos turinio filtravimo sistemos.

38. Informacinėse sistemose naudojamų interneto svetainių (toliau – svetainės) saugos valdymo reikalavimai:

38.1. svetainės turi atitikti Kibernetinio saugumo reikalavimų apraše ir Techniniuose reikalavimuose nustatytus reikalavimus;

38.2. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojo kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

38.3. turi būti pakeistos numatytos prisijungimo prie svetainių turinio valdymo sistemos (TVS) ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

38.4. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

38.5. informacinėse sistemose naudojamų svetainių sauga turi būti vertinama informacinių sistemų rizikos įvertinimo metu ir (arba) informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka.

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

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

39.2. prieiga prie informacinių sistemų suteikiama tik registruotiems informacinių sistemų naudotojams;

39.3. informacinių sistemų elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus;

39.4. informacinių sistemų elektroninė informacija viešais elektroninių ryšių tinklais perdavimas turi būti šifruojamas.

40. Informacinių sistemų elektroninės informacijos perdavimui naudojamas Savivaldybės administracijos valdomas ir kitas saugus elektroninių ryšių tinklas.

41. Visos informacinių sistemų naudotojų kompiuterizuotos darbo vietos turi būti valdomos naudojant centralizuoto valdymo priemones (pvz., katalogų tarnybą *Active direktory*).

42. Informacinių sistemų naudotojų tarnybinėms funkcijoms vykdyti naudojamuose nešiojamuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas informacinių sistemų naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas.

43. Informacinių sistemų naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie informacinių sistemų galimybė:

43.1. techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose nurodytos priemonės ir elektroninės informacijos šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN);

43.2. prie informacinių sistemų prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

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

44.1. informacinių sistemų elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną;

44.2. prireikus jas atkurti tokią teisę turi administratorius;

44.3. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas;

44.4. informacinių sistemų elektroninės informacijos kopijos saugomos kitoje patalpoje nei informacinių sistemų tarnybinės stotys.

45. Turi būti užtikrintas saugos incidentų, įvykusių informacinėse sistemose, registravimas, valdymas ir tyrimas informacinių sistemų valdytojo patvirtinta tvarka:

45.1. registruojami informacinėse sistemose įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis saugos incidentai valdomi, tiriami ir šalinami bei atkuriama sistemų veikla;

45.2. Nacionaliniam kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

46. Ne rečiau kaip kartą per savaitę turi būti atliekama informacinių sistemų naudotojų veiksmų audito įrašų analizė.

47. Ne rečiau kaip kartą per mėnesį turi būti atliekama ugniasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams nedelsiant šalinamos.

48. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

49. Perkant paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, jų projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, patalpų priežiūra, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, ją apdoroti, saugoti, keistis elektronine informacija ar tiekti informacinių technologijų infrastruktūros komponentus, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų vykdytojas ar techninės ir programinės įrangos tiekėjas (toliau – paslaugų teikėjas) privalo laikytis informacinių sistemų saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

50. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarties vykdymui, taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija (įskaitant informacinėse sistemose tvarkomą elektroninę informaciją) yra konfidenciali, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

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

52. Saugos įgaliotiniu, administratoriumi negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieneri metai.

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

54. Visi administratoriai ir naudotojai turi būti susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

55. Naudotojai, tvarkantys elektroninę informaciją, privalo įsipareigoti saugoti informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą bei valstybės tarnybos ar darbo santykius.

56. Naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, pasirašytinai supažindinami su asmens duomenų tvarkymą ir apsaugą reglamentuojančiais teisės aktais ir atsakomybe už jų pažeidimą bei raštu įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pasibaigus darbo (tarnybos) santykiams, per visą asmens duomenų teisinės apsaugos laiką, jeigu Asmens duomenų teisinės apsaugos įstatymas nenumato ko kita.

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

58. Informacinių sistemų naudotojai privalo:

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

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

58.3. įtarę, kad prisijungimo prie informacinės sistemos slaptažodis galėjo būti atskleistas kitam asmeniui, praradę ar kitaip netekę slaptažodžio, nedelsiant informuoti administratorių arba saugos įgaliotinį.

59. Informacinių sistemų naudotojams draudžiama:

59.1. atskleisti informacinės sistemos duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

59.2. savavališkai diegti informacinės sistemos taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

59.3. atskleisti kitiems asmenims prisijungimo prie informacinės sistemos vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

59.4. naudoti informacinės sistemos duomenis kitokiais nei jų nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;

59.5. sudaryti sąlygas pasinaudoti informacinei sistemai tvarkyti naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

59.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti informacinės sistemos duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo informacinės sistemos duomenis;

59.7. savavališkai prijungti prie informacinių sistemų kompiuterizuotų darbo vietų išorines duomenų laikmenas ar įrenginius, išskyrus nurodytus Saugos nuostatų 37 punkte;

59.8. atlikti bet kokius kitus neteisėtus informacinės sistemos tvarkymo veiksmus.

60. Informacinių sistemų naudotojams ne rečiau kaip kartą per kalendorinius metus turi būti rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymai organizuojami periodiškai.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

61. Tvarkyti informacinių sistemų elektroninę informaciją gali tik informacinių sistemų naudotojai, susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugą, taip pat atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose

nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

62. Informacinių sistemų naudotojų supažindinimą su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais organizuoja Savivaldybė administracijos saugos įgaliotinis.

63. Informacinių sistemų naudotojai su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą (jungiantis prie informacinės sistemos per naudotojo sąsają ar pan.).

64. Saugos nuostatai ir informacinių sistemų saugos politiką įgyvendinantys dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Informacinių sistemų saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Savivaldybės administracijos saugos įgaliotinis atsakingas, kad informacinių sistemų naudotojai būtų informuoti apie jų pakeitimą ir (ar) pripažinimą netekusiais galios.

_____

Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų priedas

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	**Informacinės sistemos pavadinimas**	Maksimalus valstybės informacinį išteklių sudarančių duomenų ar jų grupių KVP pažeidimo poveikio informacinei sistemai, kurioje jie tvarkomi, lygis	**Informacinės sistemos priskyrimo svarbos rūšiai kriterijai**
1.	Dokumentų valdymo sistema „Kontora“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu
2.	SIAIS „Parama“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu
3.	Finansų valdymo ir apskaitos informacinė sistema „BiudžetasVS“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu
4.	Viešųjų pirkimų informacinė sistema „VIPIS“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu
5.	Personalo valdymo informacinė sistema „Personalas“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu

6.	Sutarčių valdymo sistema „SVS“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu
7.	Strateginio planavimo informacinė sistema „STRAPIS“	Mažos svarbos	Valstybės informacinių išteklių svarbos vertinimas atliekamas vadovaujantis Metodikos 8.5.4. papunkčiu

_____

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2024 m. gruodžio 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 atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, kituose IS elektroninės informacijos tvarkymą ir saugą reglamentuojančiuose teisės aktuose vartojamas sąvokas.

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

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

4.1. 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;

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

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

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

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

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

4.7. IS naudotojams negali būti suteikiamos IS administratoriaus teisės;

4.8. 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

5. 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.

6. IS naudotojų įgaliojimai, teisės ir pareigos:

6.1. IS naudotojai turi teisę:

6.1.1. 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;

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

6.2. IS naudotojai privalo:

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

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

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

7. IS administratoriaus įgaliojimai, teisės ir pareigos:

7.1. administratorius yra įgaliotas ir turi teisę:

7.1.1. fiziškai prieiti prie techninės ir sisteminės programinės įrangos;

7.1.2. vykdyti informacinės sistemos techninės priežiūros funkcijas;

7.1.3. matyti visų naudotojų identifikavimo ir suteiktų teisių duomenis;

7.1.4. matyti naudotojų su tvarkomais duomenimis atliktus veiksmus;

7.1.5. atlikti užklausas informacinėje sistemoje pagal pasirinktus paieškos kriterijus.

7.2. Administratorius privalo:

7.2.1. registruoti naujus naudotojus;

7.2.2. tvarkyti esamų naudotojų duomenis;

7.2.3. konsultuoti naudotojus dėl informacinės sistemos veikimo ir kitais su informacine sistema susijusiais klausimais;

7.2.4. vykdyti kitas su informacine sistema susijusias funkcijas;

7.2.5. pagal kompetenciją užtikrinti nepertraukiamą informacinės sistemos techninės ir sisteminės programinės įrangos veikimą.

7.3. IS administratoriaus veiksmai reglamentuoti informacinės sistemos duomenų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose.

8. Saugos įgaliotinio įgaliojimai, teisės ir pareigos:

8.1. saugos įgaliotinis yra įgaliotas ir turi teisę:

8.1.1. teikti Savivaldybės administracijos direktoriui pasiūlymus dėl:

8.1.1.1. administratoriaus paskyrimo;

8.1.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

8.1.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo organizavimo;

8.2. teikti administratoriui privalomus vykdyti nurodymus ir pavedimus.

8.3. Saugos įgaliotinis privalo:

8.3.1. koordinuoti elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą;

8.3.2. kasmet organizuoti rizikos vertinimą, rengti apibendrintą rizikos vertinimo ataskaitą.

III SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

9. Saugos įgaliotinis yra atsakingas už informacinės sistemos naudotojų supažindinimą su Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatais, Šakių rajono savivaldybės administracijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis, Šakių rajono savivaldybės administracijos informacinių sistemų veiklos tęstinumo valdymo planu, šiomis Taisyklėmis ir kitais saugos politiką įgyvendinančiais teisės aktais.

10. Naudotojai su Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių dokumentų reikalavimų nesilaikymą supažindinami pasirašytinai DVS „Kontora“ priemonėmis.

IV SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

11. 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.

12. 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).

13. IS naudotojo slaptažodžiui yra keliami šie reikalavimai:

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

13.2. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;

13.3. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

14. IS naudotojas privalo:

14.1. 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);

14.2. saugoti slaptažodį ir jo neatskleisti tretiesiems asmenims;

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

15. IS administratorių slaptažodžiams yra keliami šie reikalavimai:

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

15.2. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

16. 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.

17. Didžiausias leistinas IS naudotojo mėginimų įvesti teisingą slaptažodį ne daugiau kaip 3 kartai. Tiek kartų suvedus neteisingą slaptažodį paskyra blokuojama ir informuojamas IS administratorius.

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

19. IS naudotojui teisė naudotis IS panaikinama:

19.1. pasibaigus tarnybos ar darbo santykiams;

19.2. netekus teisės naudotis IS duomenimis.

20. IS administratoriaus teisės naudotis IS sustabdoma administratoriui ilgiau kaip 2 mėnesius nesijungiant prie IS.

21. Jeigu administratorius nušalinamas nuo darbo (pareigų) ar kitaip neatitinka kituose teisės aktuose nustatytų reikalavimų, to teisė naudotis IS panaikinama nedelsiant.

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

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

23. 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 (-si) Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugą reglamentuojančių teisės aktų nuostatomis, tvarkydamas (-a) ir / ar naudodamas (-a) 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 (-a), 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
2024 m. gruodžio 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“ (toliau – Aprašas) 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 administracijos (toliau – Administracija) valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartį, naudojantiems kompiuterinę įrangą darbo užduotims atlikti.

4. Šiose Taisyklėse vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Apraše, Saugos nuostatuose ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

5. Už informacinių sistemų duomenų saugų tvarkymą atsakingi informacinių sistemų naudotojai ir informacinių sistemų administratorius.

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

7. Vadovaujantis Aprašo nuostatomis, Saugos nuostatais ir Valstybės informacinių išteklių įstatymo 3 straipsniu, informacinė sistema priskiriama mažos svarbos valstybės informacinių išteklių rūšiai.

8. Informacinėje sistemoje tvarkoma elektroninė informacija yra skirstoma į šias grupes:

8.1. informacinės sistemos administratoriaus tvarkoma elektroninė informacija;

8.2. informacinės sistemos naudotojų tvarkoma elektroninė informacija.

9. Informacinės sistemos elektroninės informacijos, priskirtos šių Taisyklių 8 punkte nurodytoms grupėms, sąrašas:

9.1. informacinės sistemos administratoriaus tvarkoma elektroninė informacija:

9.1.1. informacinės sistemos naudotojų teisės;

9.1.2. informacinės sistemos techninės ir programinės įrangos parametrai;

9.1.3. informacinės sistemos naudotojų veiksmų registravimo duomenys;

9.1.4. informacinės sistemos rezervinės kopijos;

9.2. informacinės sistemos naudotojų tvarkoma elektroninė informacija:

9.2.1. informacinės sistemos duomenų bazėje kaupiami duomenys ir funkcijos pagal suteiktas teises;

9.2.2. informacinės sistemos naudotojo parametrai.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

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

11. Naudojama legali sisteminė ir taikomoji programinė įranga.

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

13. 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.

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

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

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

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

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

19. Saugiam elektroninės informacijos teikimui ir (ar) gavimui iš kitų valstybės institucijų užtikrinti naudojamas Saugus valstybės duomenų perdavimo tinklas (toliau – SVDPT). Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.

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

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

22. Fizinė prieiga prie informacinių sistemų tarnybinių stočių suteikiama tik informacinių technologijų darbuotojams.

23. 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. Svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 minučių.

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

25. Tarnybinių stočių patalpoje įrengta oro kondicionavimo sistema.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

26. Informacinių sistemų duomenų keitimą, atnaujinimą ir naujų duomenų įvedimą turi teisę atlikti tik autorizuoti naudotojai, turintys teisę tai atlikti.

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

28. Už informacinių sistemų duomenų atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsako Administratorius.

29. Auditui atlikti turi būti fiksuojama ši informacija:

29.1. informacinės sistemos elementų įjungimas, išjungimas ar perkrovimas (jeigu informacinės sistemos dalys palaiko tokį funkcionalumą);

29.2. informacinės sistemos naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti), atsijungimas;

29.3. audito funkcijos įjungimas, išjungimas;

29.4. audito įrašų trynimas, kūrimas ar keitimas.

30. Kiekviename audito duomenų įraše turi būti fiksuojama:

30.1. įvykio data ir tikslus laikas;

30.2. informacinės sistemos naudotojo / administratoriaus ir (arba) informacinės sistemos įrenginio, susijusio su įvykiu, duomenys;

30.3. įvykio rezultatas.

31. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

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

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

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

35. Atstatymų išbandymą inicijuoja Saugos įgaliotinis.

36. Duomenų perkėlimo ir teikimo kitoms informacinėms sistemoms bei duomenų gavimo iš jų tvarka nustatoma atskiromis sutartimis.

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

38. Operacinių sistemų ir taikomosios programinės įrangos pakeitimai turi būti valdomi: planuojami ir ištestuojami, numatomos atstatomosios procedūros nesėkmingų pakeitimų atvejams, įvertinamas pakeitimų poveikis saugumui.

39. Informacinių sistemų pakeitimų valdymo tvarka nustatyta šių Taisyklių priede „Šakių rajono savivaldybės administracijos informacinių sistemų pakeitimų valdymo tvarkos aprašas“.

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

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

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

43. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau – mobilieji įrenginiai), naudojamų informacinės sistemos naudotojų tarnybinėms ar darbo funkcijos vykdyti, naudojimo tvarka:

43.1. išnešti iš informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpų mobilieji įrenginiai negali būti palikti be priežiūros viešose vietose; kelionės metu mobilieji įrenginiai turi būti saugomi;

43.2. iš informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpų išnešamiems mobiliesiems įrenginiams turi būti taikomos papildomos saugos priemonės:

43.2.1. elektroninė informacija turi būti šifruojama;

43.2.2. teisė naudotis įrenginiu suteikiama tik Administracijos darbuotojams;

43.2.3. įrenginys, baigus juo naudotis, turi būti užrakinamas;

43.2.4. prisijungimas gali būti ribojamas naudojant naudotojo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

43.2.5. turi būti užtikrinta kompiuterinių laikmenų apsauga – jei yra techninių galimybių, duomenys turi būti šifruojami tiek mobiliųjų įrenginių laikmenose, tiek išorinėse

kompiuterinėse laikmenose. Draudžiama saugoti neužšifruotose mobiliųjų įrenginių laikmenose konfidencialią ir (arba) asmens duomenų informaciją;

43.2.6. mobilusis įrenginys, kuriuo nesinaudojama 10 minučių, turi automatiškai užsirakinti;

43.2.7. mobilusis įrenginys, prieš perduodant jį Administracijos darbuotojui, turi būti patikrinamas antivirusine programine įranga;

43.3. duomenys, perduodami tarp mobiliojo įrenginio ir informacinės sistemos, turi būti šifruojami;

43.4. turi būti užtikrinta kompiuterinių laikmenų apsauga, t. y. esant techninėms galimybėms turi būti šifruojami duomenys tiek mobiliųjų įrenginių laikmenose, tiek išorinėse kompiuterinėse laikmenose. Draudžiama saugoti neužšifruotuose mobiliųjų įrenginių laikmenose konfidencialią ir (arba) asmens duomenų informaciją;

43.5. už mobiliųjų įrenginių ir jame tvarkomų ar saugomų duomenų saugą teisės aktų nustatyta tvarka atsako naudotojas, kuriam šis įrenginys yra skirtas.

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

44. Administratorius suteikia prieigos prie informacinių sistemų 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.

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

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

47. Reikalavimai informacinėms sistemoms, reikalingoms paslaugų teikėjams ir jų projektavimo, aptarnavimo ir priežiūros teikiamoms paslaugoms funkcionuoti nustatomi šių paslaugų teikimo sutartyse.

48. 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“

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

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

49.2. sertifikuotą sisteminę programinę įrangą, atitinkančią kibernetinio saugumo reikalavimus, nustatytus Lietuvos Respublikos Vyriausybės patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

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

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

Šakių rajono savivaldybės
administracijos saugaus elektroninės
informacijos tvarkymo taisyklių
priedas

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ PAKEITIMŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šakių rajono savivaldybės administracijos informacinės sistemos pakeitimų valdymo tvarkos aprašas (toliau – Aprašas) nustato standartizuotą funkcinių, techninių, programinių, organizacinių ir administracinių Šakių rajono savivaldybės administracijos (toliau – Administracija) informacinių sistemų (toliau – informacinės sistemos) pakeitimų valdymą ir kontrolę, siekiant sumažinti neigiamo pakeitimų poveikio informacinių sistemų darbui riziką, užtikrinant saugų ir kokybišką reikalingų pakeitimų įvykdymą.

2. Apraše vartojamos sąvokos, kaip jos apibrėžtos Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“, Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatuose ir kituose teisės aktuose.

II SKYRIUS
PAKEITIMŲ IDENTIFIKAVIMAS

3. Pakeitimai identifikuojami analizuojant informacinių sistemų valdytojo ir tvarkytojų veiklos aplinką ir poreikius, kuriuos formuoja technologiniai aspektai ir tendencijos, esama padėtis (informacinės sistemos sąranka, pažeidžiamumas, atitiktis teisės aktų ir standartų reikalavimams ir pan.).

4. Pakeitimai identifikuojami pagal pakeitimo tipą: administraciniai, organizaciniai ar techniniai.

III SKYRIUS
PAKEITIMŲ INICIJAVIMAS IR SKIRSTYMAS Į KATEGORIJAS

5. Pakeitimus inicijuoti turi teisę informacinių sistemų valdytojas, informacinės sistemos tvarkytojai, informacinės sistemos saugos įgaliotinis (toliau – saugos įgaliotinis) ir (ar) informacinės sistemos administratorius (toliau – administratorius).

6. Registruojami pakeitimai, atsižvelgiant į jų svarbą, aktualumą ir poreikį, skirstomi į šias kategorijas:

6.1. standartiniai pakeitimai, kurie nekelia rizikos kokybiškam elektroninių paslaugų teikimui arba visos informacinių technologijų infrastruktūros veikimui (pvz., naujos kompiuterinės darbo vietos parengimas informacinės sistemos naudotojui ar informacinės sistemos komponentų pakeitimas, standartinės programinės įrangos įdiegimas, atnaujinimas ar išdiegimas, saugumo spragų

pataisų įdiegimas informacinės sistemos naudotojo kompiuterinėje darbo vietoje ir pan.);

6.2. skubūs pakeitimai, kurie skirti aukščiausio prioriteto sutrikimams arba problemoms šalinti ir reikalauja ypatingos įvertinimo, patvirtinimo ir atlikimo skubos, taip pat avariniai pakeitimai (pvz., veiklos atkūrimas likviduojant informacinės sistemos elektroninės informacijos (toliau – elektroninė informacija) saugos ar kibernetinio incidento, stichinės nelaimės, avarijos ar kitų ekstremalių situacijų padarinius);

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

7. Prioritetas turi būti skiriamas skubiems ir plėtros (vystymo) pakeitimams. Pakeitimų prioritetas nustatomas pakeitimų įtakos vertinimo metu.

IV SKYRIUS
PAKEITIMŲ ĮTAKOS VERTINIMAS

8. Informacinių sistemų funkcinių, programinių ir techninių pakeitimų įtaką pagal kompetenciją vertina Administracijos Bendrųjų reikalų skyrius. Sudėtingų pakeitimų įtakai įvertinti iš informacinių sistemų valdytojo kompetentingų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis (toliau – darbuotojai), prireikus – iš nepriklausomų ekspertų gali būti sudaroma darbo grupė.

9. Pakeitimų įtakos vertinimo metu turi būti įvertinama pakeitimų nauda, pagrįstumas, įgyvendinamumas, pakeitimams atlikti reikalingos sąnaudos, taip pat informacinių sistemų darbo sutrikdymo ar sustabdymo rizika, elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo pažeidimo rizika.

10. Administracijos programinės ir techninės įrangos pakeitimai atliekami tik įvertinus pakeitimo poreikį, pakeitimo apimtį ir sistemos modernizavimo mastą.

V SKYRIUS
PAKEITIMŲ ATLIKIMAS

11. Techninius informacinės sistemos pakeitimus vykdo administratorius arba paslaugos teikėjas. Organizacinius ir administracinius pakeitimus vykdo Administratorius arba paslaugos teikėjas .

12. Visi pakeitimai, galintys sutrikdyti ar sustabdyti informacinių sistemų darbą, turi būti suderinti su saugos įgaliotiniu ir vykdomi tik gavus jo pritarimą.

13. Pakeitimai, galintys sutrikdyti ar sustabdyti informacinių sistemų darbą, daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri yra atskirta nuo eksploatuojamų informacinių sistemų. Eksploatuojamų informacinių sistemų aplinkoje pakeitimai gali būti vykdomi tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių (pvz., veiklos atkūrimo ar kitos avarinės situacijos) nėra galimybės jų patikrinti bandomojoje informacinės sistemos aplinkoje.

14. Nustačius, kad informacinės sistemos pakeitimai bandomojoje aplinkoje rezultatas atitinka laukiamus rezultatus, pakeitimai gali būti atliekami eksploatuojamos informacinės sistemos aplinkoje. Nustatytu darbo laiku gali būti vykdomi tik skubūs ir standartiniai pakeitimai.

15. Informacinės sistemos administratorius turi informuoti informacinės sistemos naudotojus, informacinių sistemų tvarkytojus, kitus suinteresuotus asmenis apie pakeitimus, kuriuos įgyvendinant galimi informacinės sistemos darbo sutrikimai. Apie pakeitimus naudotojai informuojami elektroniniu paštu ne vėliau kaip likus vienai darbo dienai iki planuojamo pakeitimo įgyvendinimo pradžios. Šis punktas netaikomas, jeigu įgyvendinami skubūs pakeitimai.

VI SKYRIUS
PAKEITIMŲ VALDYMO PROCESAS

16. Pakeitimų valdymo procesas vykdomas atsižvelgiant į Aprašo, Informacinių technologijų paslaugų valdymo metodikos, patvirtintos Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013 m. birželio 19 d. įsakymu Nr. T-83 „Dėl Informacinių technologijų paslaugų valdymo metodikos patvirtinimo“, reikalavimus.

_____

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2024 m. gruodžio d.
įsakymu Nr.

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS 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. pavaduotojas – informacinių sistemų administratorius;

8.3. grupės nariai:

8.3.1. administracijos direktorius;

8.3.2. Bendrųjų reikalų skyriaus vedėjas;

8.3.3. Administracijos patarėjas (parengties pareigūnas).

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. pavaduotojas – informacinių sistemų administratorius;

10.3. grupės nariai:

10.3.1. kompiuterinių tinklų administratorius;

10.3.1. 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. Įvykus elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma informacinės sistemos techninė ir programinė įranga, atliekami veiksmai:

12.1. informacinės sistemos administratorius nedelsdamas informuoja apie nenumatytą situaciją saugos įgaliotinį;

12.2. saugos įgaliotinis apie elektroninės informacijos saugos incidentą nedelsdamas informuoja informacinės sistemos naudotojo padalinio vadovą;

12.3. saugos įgaliotinis informaciją įrašo į Šakių rajono savivaldybės administracijos informacinių sistemų elektroninės informacijos saugos incidentų registravimo žurnalą (3 priedas), vadovauja veiklos tęstinumo valdymo detaliajame plane (1 priedas) nurodytiems veiksmams;

12.4. informacinių sistemų administratorius atkuria tarnybinės stoties, kompiuterių tinklo veiklą, duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja informacinės sistemos naudotojo padalinio vadovą bei saugos įgaliotinį;

12.5. saugos įgaliotinis kartu su administratoriumi organizuoja žalos informacinių sistemų duomenims, techninei bei programinei įrangai vertinimą, koordinuoja informacinių sistemų veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą.

13. Nesant galimybių tęsti veiklą pagrindinėse informacinės sistemos patalpose, informacinės sistemos įranga per 1 dieną laikinai perkeliama į atsargines patalpas, kurias užtikrina Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka pasirinktas paslaugų teikėjas.

14. Atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti saugumo incidento atveju, keliami šie reikalavimai:

14.1. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

14.2. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės;

14.3 ryšio įranga turi būti apsaugota nuo nesankcionuoto prisijungimo.

15. Elektroninės informacijos saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka panaudojant Savivaldybės biudžeto išteklius ar kitus finansavimo šaltinius.

16. Veiklos tęstinumo valdymo grupė ir veiklos atkūrimo grupė tarpusavyje bendrauja elektroniniu paštu ir (ar) telefonu. Ne rečiau negu kartą per metus Veiklos tęstinumo valdymo grupės vadovas arba jo pavedimu – Veiklos tęstinumo valdymo grupės narys organizuoja šių grupių susitikimą, kuriame aptariama esama Informacinės sistemos situacija.

17. Įvykus kibernetiniam incidentui Savivaldybės administracijos informacinėje sistemoje, Nacionalinį kibernetinio saugumo centrą informuoti apie:

17.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;

17.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;

17.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

18. Kibernetinius incidentus pavojingo incidento kategorijai turi teisę priskirti tik Nacionalinis kibernetinio saugumo centras.

19. Kriterijai, kuriais vadovaujantis kibernetiniai incidentai priskiriami 17.1–17.3 papunkčiuose nustatytoms kategorijoms, yra nustatyti Nacionalinio kibernetinių incidentų valdymo plano priede.

20. Informuoti apie kibernetinius incidentus Savivaldybės administracijos informacinėje sistemoje Nacionalinį kibernetinį saugumo centrą Nacionalinio kibernetinio saugumo centro interneto svetainėje nurodytais kontaktais. Už pranešimą Nacionaliniam kibernetinio saugumo centrui ir taikytas kibernetinių incidentų tyrimo ar valdymo priemones yra atsakingas Informacinės sistemos saugos įgaliotinis.

21. Savivaldybės administracija kibernetinių incidentų tyrimą atlieka vadovaudamasi savo patvirtintais saugumo teisės aktais tiek, kiek to nereglamentuoja Nacionalinio kibernetinių incidentų valdymo planas, ir imasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai informacinės sistemos veiklai atkurti.

22. Informacinių sistemų saugos įgaliotinis Nacionaliniam kibernetinio saugumo centrui pateikia kibernetinio incidento tyrimo ataskaitą apie:

22.1. didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per keturias valandas nuo jų nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

22.2. vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per dvidešimt keturias valandas nuo jų nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

22.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo.

23. Nacionaliniam kibernetinio saugumo centrui teikiant didelio ar vidutinio poveikio kibernetinio incidento tyrimo ataskaitą, nurodoma kibernetinio saugumo subjektui žinoma informacija:

23.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Nacionalinio kibernetinių incidentų valdymo plano priede pateiktus kriterijus;

23.2. ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, tarnybinė stotis ir panašiai);

23.3. kibernetinio incidento veikimo trukmė;

23.4. kibernetinio incidento šaltinis;

23.5. kibernetinio incidento požymiai;

23.6. kibernetinio incidento veikimo metodas;

23.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

23.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

23.9. kibernetinio incidento būsena (aktyvus, pasyvus);

23.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

23.11. galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės;

23.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Nacionalinio kibernetinių incidentų valdymo plano 23 punktu.

24. Informacinės sistemos saugos įgaliotinis, įvertinęs, kad negalės savarankiškai ištirti ar suvaldyti kibernetinio incidento per maksimaliai leistiną paslaugos neveikimo laiką, nustatytą savo patvirtintuose kibernetinio saugumo teisės aktuose, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo kreipiasi pagalbos į Nacionalinį kibernetinio saugumo centrą.

25. Didelio ar vidutinio poveikio kibernetinių incidentų tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta kibernetinio incidento poveikis ryšių ir informacinei sistemai ir (ar) atkuriama įprasta ryšių ir informacinės sistemos veikla, atitinkanti kriterijus, nurodytus 8 punkte.

26. Informacinių sistemų saugos įgaliotinis ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo informuoja ryšių ir informacinės sistemos teikiamų paslaugų gavėjus (jeigu tokių yra), jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos ryšių ir informacinės sistemos teikiamų paslaugų gavėjui.

27. Informacinės sistemos saugos įgaliotinis ir (ar) Savivaldybės administracijos direktoriaus paskirti darbuotojai po kibernetinio incidento suvaldymo ar pasibaigimo pagal kompetenciją atlieka jo analizę. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

28. Informacinių sistemų saugos įgaliotinis, išanalizavęs ir įvertinęs visą informaciją, susijusią su kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

28.1 ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikia kibernetinio incidento analizės rezultatus Nacionaliniam kibernetinio saugumo centrui ir kibernetinio saugumo informaciniame tinkle paskelbia susistemintą ir aktualią neįslaptintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą;

28.2. imasi priemonių, kad būtų pašalintas ryšių ir informacinės sistemos pažeidžiamumas;

28.3. įvertina ryšių ir informacinių sistemų riziką ir atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

28.4. nustačius teisinio reglamentavimo spragų, pakeičia savo kibernetinio saugumo teisės aktus ir (ar) inicijuoja kitų institucijų priimtų teisės aktų pakeitimus.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

29. Parengtų saugomų dokumentų sąrašas:

29.1. 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;

29.2. 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;

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

29.4. 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;

29.5. 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;

29.6. 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.

30. Valdymo plano 29 punkte nurodytų dokumentų kopijas saugo sistemos duomenų valdymo įgaliotinis.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

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

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

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

34. Valdymo plano išbandymo ataskaitos ne vėliau kaip per penkias darbo dienas, nuo šių dokumentų priėmimo dienos, pateikiamos Nacionaliniam kibernetinio saugumo centrui.

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

_____

Informacinių sistemų veiklos tęstinumo valdymo
plano
1 priedas

INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Įvykis, sukeliantis elektroninės informacijos saugos incidentą	**Pasekmės likvidavimo veiksmai**	**Vykdymo terminai**	**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;	Nedelsiant pastebėjus	Pavojų pastebėjęs darbuotojas
	1.1.2. pranešti specialiosioms tarnyboms;	1 val.	Veiklos tęstinumo valdymo grupės vadovas
	1.1.3. iškviesti Veiklos tęstinumo valdymo grupės narius į saugią vietą;	1 val.	
	1.1.4. informuoti sistemos veiklos atkūrimo grupės vadovą;	1 val.	
	1.1.5. iškviesti sistemos veiklos atkūrimo grupės narius į saugią vietą;	3 val.	Veiklos atkūrimo grupės vadovas
	1.1.6. vykdyti specialiųjų tarnybų nurodymus;		Visi darbuotojai
	1.1.7. organizuoti darbuotojų evakuaciją, suskaičiuoti evakuotus darbuotojus;	1 val.	Veiklos tęstinumo valdymo grupė
	1.1.8. informuoti specialiąsias tarnybas apie dingusius darbuotojus;	Nedelsiant	
	1.1.9. gavus rekomendacijas iš specialiųjų tarnybų, informuoti darbuotojus, kaip elgtis esant susidariusiai situacijai;	Nedelsiant	

	1.1.10. esant būtinybei, išjungti ir užrakinti visą	1 val.	Veiklos atkūrimo grupė
	1.1.11. įvertinti pažeidimus ir padarytus nuostolius;	24 val.	
	1.1.12. informuoti darbuotojus apie darbo funkcijų vykdymo aplinkybes;	24 val.	Veiklos tęstinumo valdymo grupė
	1.1.13. nustatyti, ar buvo prarasta įranga;	24 val.	Veiklos atkūrimo grupė
	1.1.14. įrangos praradimo atveju informuoti veiklos tęstinumo valdymo grupę;	24 val.	
	1.1.15. vykdyti teisėsaugos organų ir (arba) draudimo įmonės nurodymus, pateikiant	Nedelsiant	Veiklos tęstinumo valdymo grupė
	1.1.16. esant poreikiui perskirstyti, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų atkurtas sistemos veikimas;	24 val.	
	1.1.17. trūkstant išteklių, kreiptis į sistemos valdytoją dėl papildomų resursų skyrimo;	24 val.	
	1.1.18. įsigijus įrangą, atkurti sistemos veikimą.	48 val.	Veiklos atkūrimo grupė
1.2. Paslaugos teikėjo, kurio patalpose yra sistemos programinė įranga, patalpos	1.2.1. nustačius sistemos programinės įrangos pažeidimus arba praradimą,	1 val.	Veiklos atkūrimo grupės vadovas
	1.2.2. vadovaujantis paslaugos teikimo sutartyje nustatytais įsipareigojimais, vykdyti sistemos programinės įrangos atkūrimo	Pagal sutartinius įsipareigojimus	Paslaugos teikėjas
2. Gaisras 2.1. Šakių rajono savivaldybės administracijos patalpose	2.1.1. pastebėjus gaisro židinį, stengtis jį užgesinti kuo greičiau;	Nedelsiant	Pavojų pastebėjęs darbuotojas
	2.1.2. jeigu būtina, skelbti pavojų ir pranešti priešgaisrinei gelbėjimo tarnybai;	Nedelsiant	
	2.1.3. informuoti Veiklos tęstinumo valdymo grupės	1 val.	

	vadovą;		
	2.1.4. iškviesti Veiklos tęstinumo valdymo grupę į	1 val.	Veiklos tęstinumo valdymo grupės vadovas
	2.1.5. informuoti veiklos atkūrimo grupės vadovą;	1 val.	
	2.1.6. iškviesti veiklos atkūrimo grupę;	3 val.	Veiklos atkūrimo grupės vadovas
	2.1.7. vykdyti specialiųjų tarnybų nurodymus;	Nedelsiant	Visi darbuotojai
	2.1.8. jeigu būtina, organizuoti darbuotojų evakuaciją, suskaičiuoti evakuotus darbuotojus;	1 val.	Veiklos tęstinumo valdymo grupė
	2.1.9. informuoti specialiąsias tarnybas apie dingusius darbuotojus;	3 val.	
	2.1.10. gavus rekomendacijas iš specialiųjų tarnybų, informuoti darbuotojus, kaip elgtis	Nedelsiant	
	2.1.11. likvidavus gaisrą įvertinti pažeidimus ir	24 val.	Veiklos atkūrimo grupė
	2.1.12. esant poreikiui perskirstyti, kiek tai yra įmanoma, turimus rezervinius išteklius, kad būtų	24 val.	Veiklos tęstinumo valdymo grupė
	2.1.13. nesant pakankamam rezervui, kreiptis į sistemos valdytoją dėl papildomų resursų skyrimo;	24 val.	
	2.1.14. įsigijus įrangą, atkurti sistemos veikimą.	48 val.	Veiklos atkūrimo grupė
2.2. Paslaugos teikėjo, kurio patalpose yra sistemos programinė įranga, patalpos	2.2.1. nustačius sistemos programinės įrangos pažeidimus arba praradimą	1 val.	Paslaugos teikėjas
	2.2.2. vadovaujantis paslaugos teikimo sutartyje nustatytais įsipareigojimais vykdyti sistemos programinės įrangos atkūrimo	Pagal sutartinius įsipareigojimus	Paslaugos teikėjas
3. Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų funkcionalumui	3.1. informuoti sistemos valdytoją;	1 val.	Veiklos tęstinumo valdymo grupė
	3.2. vykdyti sistemos programinės įrangos atkūrimo darbus.	3 val.	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;	3 val.	Veiklos tęstinumo valdymo grupė
	4.2. informuoti sistemos naudotojus, jeigu tai sukelia veiklos sutrikimus;	3 val.	
	4.3. jeigu sistemos duomenys prarasti ar jie tapo prieinami tam leidimo neturintiems asmenims, pranešti teisėsaugos organams;	3 val.	
	4.4. vykdyti teisėsaugos organų nurodymus, pateikiant reikiamą informaciją apie įvykį;	6 val	
	4.5. atkurti sistemos darbingumą;	24 val.	Veiklos atkūrimo grupė
	4.6. nustatyti, ar atkurti duomenys yra patikimi;	24 val.	Veiklos atkūrimo grupė
	4.7. jeigu duomenys buvo prarasti dėl saugumo spragų, pašalinti jas;	24 val.	
	4.8. atkurti sistemos duomenis iš paskutinės geros atsarginės kopijos;	48 val.	
	4.9. visiškai atkurti sistemos veiklą ir visas sistemos naudotojų galimybes naudotis sistema.	48 val.	
5. Sistemos veiklos sutrikdymas dėl kibernetinių atakų	5.1. nutraukti paslaugų teikimą sistemos naudotojams ir informuoti juos apie veiklos sutrikimus;	3 val.	Veiklos atkūrimo grupė
	5.2. nustatyti trikdžių šaltinį;	8 val.	
	5.3. pranešti elektroninių ryšių ir informacijos saugumo incidentų tyrimo tarnyboms,	8 val.	Veiklos tęstinumo valdymo grupė
	5.4. patikrinti, ar neprarasti arba nesugadinti	8 val.	Veiklos atkūrimo grupė

	5.5. pašalinti trikdžius, atkurti sistemos veikimą.	24 val.	Veiklos atkūrimo grupė
6. Elektros ir telekomunikacinių ryšių tiekimo sutrikimai	6.1. jeigu yra galimybė, nustatyti elektros ir ryšių paslaugų teikimo sutrikimo priežastis;	3 val.	Veiklos tęstinumo valdymo grupė
	6.2. kreiptis į paslaugų teikėją dėl sutrikimų pašalinimo;	3 val.	
	6.3. informuoti darbuotojus ir pateikti rekomendacijas, kaip elgtis esant susidariusiai situacijai;	3 val.	
	6.4. pašalinus sutrikimą, atnaujinti sistemos	24 val.	Veiklos atkūrimo grupė
7. Vandentiekio ar šildymo sistemos avarija	7.1. kreiptis į specialiąsias tarnybas dėl sutrikimų pašalinimo;	3 val.	Veiklos tęstinumo valdymo grupė
	7.2. informuoti darbuotojus ir pateikti rekomendacijas, kaip elgtis esant susidariusiai situacijai;	3 val.	
	7.3. pašalinus sutrikimą, atnaujinti sistemos	24 val.	Veiklos atkūrimo grupė

_____

Informacinių sistemų 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)

Informacinių sistemų veiklos tęstinumo
valdymo plano
3 priedas

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20___m._____d.

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	IS naudotojo padalinio pavadinimas	**Požymio kodas**	**Įvykio aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Pašalino (vardas, pavardė)**	**Saugos įgaliotinis (vardas, pavardė, parašas)**
1.							
2.							
3.							
4.							
5.							
6.							

Elektroninės informacijos saugos incidento situacijos požymiai:
1. Gamtos veiksniai. 2. Gaisras. 3. Patalpai padaryta žala arba patalpos praradimas. 4. Energijos tiekimo sutrikimai. 5. Vandentiekio ir šildymo sistemos sutrikimai; 6. Ryšio sutrikimai. 7. Tarnybinių stočių sugadinimas ir (arba) praradimas. 8. Programinės įrangos sugadinimas, praradimas. 9. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas. 10. Įvykiai, susiję su teroristine veikla. 11. Informacinės sistemos veiklos sutrikdymas dėl kibernetinių atakų

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Šakių rajono savivaldybės administracija
Dokumento pavadinimas (antraštė)	Dėl Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų, informacinių sistemų naudotojų administravimo taisyklių, saugaus elektroninės informacijos tvarkymo taisyklių, informacinių sistemų veiklos tęstinumo valdymo plano patvirtinimo
Dokumento registracijos data ir numeris	2024-12-30 Nr. AT-933
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	Vytautas Ižganaitis Administracijos direktorius
Parašo sukūrimo data ir laikas	2024-12-30 16:39
Parašo formatas	Einamojo galiojimo (XAdES-EPES)
Laiko žymoje nurodytas laikas	
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA ECC
Sertifikato galiojimo laikas	2024-07-30 08:15 - 2028-07-29 08:15
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)	Nauji duomenų saugos nuostatai.docx
Pridedamo dokumento registracijos data ir numeris	-
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	informacinių sistemų naudotojų administravimo taisyklės (1).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 (1).docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20241217.3
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2024-12-30)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2024-12-30 nuorašą suformavo Irena Bacevičienė
Paieškos nuoroda	-
Papildomi metaduomenys	-