PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2023 m. birželio 28 d.
įsakymu Nr. AV-488

SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖJE SISTEMOJE TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Saugaus elektroninės informacijos tvarkymo Rokiškio rajono savivaldybės administracijos (toliau – Administracija) informacinėje sistemoje (toliau – informacinė sistema) taisyklių (toliau – Tvarkymo taisyklės) tikslas – nustatyti informacinės sistemos naudotojų, administratoriaus, saugumo įgaliotinio veiksmus, užtikrinančius saugų informacinės sistemos techninės ir programinės įrangos funkcionavimą, duomenų tvarkymą ir teikimą duomenų gavėjams.

2. Tvarkymo taisyklės parengtos vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)“ ir LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)“, taip pat kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą, duomenų tvarkytojų veiklą ir duomenų saugumo valdymą.

Asmens duomenys tvarkomi vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, 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, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

3. Tvarkymo taisyklėse vartojamos sąvokos:

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

Elektroninė informacija (toliau – informacija) – visa informacija, kuri tvarkoma informacinių technologijų priemonėmis. Tai programos, failai ir kita informacija, kuri saugoma, perduodama ir sukuriama kompiuteriu.

Informacinės sistemos saugumo įgaliotinis (toliau – saugumo įgaliotinis) – informacijos saugumą informacinėje sistemoje įgyvendinantis valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį.

Informacinės sistemos administratorius (toliau – sistemos administratorius) – informacinės sistemos priežiūrą atliekantis valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį.

Informacinės sistemos naudotojai – Savivaldybės tarybos nariai, Kontrolės ir audito tarnybos, Savivaldybės administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį.

Informacijos tvarkymas – visos su informacija atliekamos operacijos: rinkimas, užrašymas, klasifikavimas, grupavimas, kaupimas, saugojimas, keitimas, kopijavimas, sujungimas, atskleidimas, teikimas, naudojimas, naikinimas.

Kompiuterinė įranga – kompiuteriai, serveriai, jų dalys, išoriniai įrenginiai (monitoriai, skeneriai, spausdintuvai, klaviatūros, pelės, garso kolonėlės, kompiuterių tinklo įranga, kompiuterinės bei tinklinės įrangos montavimo spintos, nepertraukiamo elektros maitinimo šaltiniai ir pan.).

Kompiuterių tinklas – serveriai ir darbo vietų kompiuteriai, kompiuterine įranga (kabeliais ir kompiuterių tinklo aparatūra) sujungti į sistemą, siekiant užtikrinti operatyvų pasikeitimą informacija, kolektyvinį kompiuterinės ir programinės įrangos naudojimą ir interneto paslaugas.

4. Visa Rokiškio rajono savivaldybės administracijos tvarkoma elektroninė informacija yra priskiriama *mažiausios* svarbos informacijos kategorijai.

5. Rokiškio rajono savivaldybės administracijos saugoma elektroninė informacija yra skirstoma į šias grupes:

5.1. Rokiškio rajono savivaldybės administracijos informacinių sistemų administratoriaus tvarkoma informacija;

5.2. Rokiškio rajono savivaldybės administracijos informacinių sistemų naudotojų tvarkoma informacija.

6. Kitos Tvarkymo taisyklėse vartojamos sąvokos suprantamos taip, kaip apibrėžtos Rokiškio rajono savivaldybės informacinės sistemos duomenų saugumo nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose bei standartuose.

II. TECHNINIŲ IR KITŲ SAUGUMO PRIEMONIŲ APRAŠYMAS

7. Kompiuterinės įrangos saugumo priemonės:

7.1. Informacinės sistemos serveriuose ir informacinės sistemos naudotojų kompiuteriuose yra įdiegta ir reguliariai atnaujinama kenksmingos programinės įrangos aptikimo bei šalinimo programinė įranga (toliau – antivirusinė įranga). Informacinės sistemos naudotojų kompiuteriuose naudojama centralizuotai valdoma antivirusinė įranga, skirta tikrinti kompiuterius ir keičiamąsias laikmenas.

7.2. Nuolat stebima informacinės sistemos serverių, duomenų perdavimo tinklo mazgų ir ryšio linijų techninė būklė.

7.3. Yra įgyvendintos gamintojo nustatytos kompiuterinės įrangos darbo sąlygos.

7.4. Informacinės sistemos serveriams apsaugoti nuo elektros srovės svyravimų yra naudojamas nepertraukiamo maitinimo šaltinis su automatine apsauga.

8. Informacinės sistemos sisteminės ir taikomosios programinės įrangos saugumo užtikrinimo priemonės:

8.1. Naudojama legali sisteminė ir taikomoji programinė įranga.

8.2. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik Administracijos informacinių technologijų specialistai.

8.3. Programinė įranga prižiūrima laikantis gamintojo rekomendacijų.

8.4. Programinei įrangai ir duomenims apsaugoti naudojamos programinės priemonės: tinklo užkardos ir elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės.

9. Administracijos patalpų, kuriose yra informacinės sistemos serveriai, saugumo užtikrinimas:

9.1. Asmenys, nesusiję su informacinės sistemos administravimu, patekti į šias patalpas gali tik lydimi sistemos administratoriaus arba jį pavaduojančio darbuotojo.

9.2. Patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės.

9.3. Patalpos atskirtos nuo bendrojo naudojimo patalpų, durys rakinamos.

9.4. Įrengta bendro naudojimo patalpų durų fizinė apsauga.

10. Kitos priemonės, naudojamos siekiant užtikrinti informacinės sistemos informacijos saugumą:

10.1. Informacinės sistemos priežiūros funkcijos atliekamos naudojant sistemos administratoriaus identifikatorių, kuris žinomas tik sistemos administratoriui ar jį pavaduojančiam darbuotojui.

10.2. Kiekvienas informacinės sistemos naudotojas unikaliai identifikuojamas – patvirtina savo tapatybę informacinės sistemos naudotojo vardu ir slaptažodžiu.

10.3. Baigęs darbą, informacinės sistemos naudotojas turi užtikrinti, kad su informacija negalėtų susipažinti pašaliniai asmenys: uždaryti programinę įrangą, įjungti ekrano užsklandą su slaptažodžiu, atsijungti nuo informacinės sistemos.

10.4. Informacinės sistemos posistemių įvykių žurnaluose registruojami informacinės sistemos naudotojų veiksmai su duomenimis, jei informacinės sistemos posistemiuose yra numatyta tokia galimybė.

III. SAUGUS INFORMACIJOS TVARKYMAS

11. Informacinės sistemos duomenų vientisumui užtikrinti, informacinės sistemos naudotojų tapatybei nustatyti ir prieigai kontroliuoti naudojama prisijungimo vardų, slaptažodžių ir prieigos teisių sistema.

12. Informacinės sistemos naudotojai identifikuojami pagal informacinės sistemos naudotojų vardus ir slaptažodžius, kurių kontrolę atlieka kompiuterio ir serverių operacinės sistemos.

13. Informacinės sistemos posistemiuose duomenis keisti, atnaujinti, įvesti naujus duomenis ir naikinti gali informacinės sistemos naudotojai, kuriems suteiktos tokios teisės.

14. Informacinės sistemos naudotojų veiksmų registravimas:

14.1. Informacinės sistemos naudotojų tapatybė ir veiksmai su informacinės sistemos posistemių duomenimis ar bandymai juos atlikti registruojami programiniu būdu informacinės sistemos posistemių įvykių žurnaluose, jei informacinės sistemos posistemiuose, kuriuose duomenys yra tvarkomi, yra tokia galimybė.

14.2. Informacinės sistemos posistemių įvykių žurnalų informacija prieinama tik administratoriams ir informacinės sistemos naudotojams, turintiems prieigos teisę prie informacinės sistemos posistemių įvykių žurnalų, jei informacinės sistemos posistemiuose, kuriuose duomenys yra tvarkomi, yra tokia galimybė.

14.3. Informacinės sistemos posistemių įvykių žurnalų įrašai suteikia galimybę nustatyti nesankcionuoto poveikio šaltinį, laiką ir veiksmus informacinės sistemos posistemių duomenims.

14.4. Informacinės sistemos naudotojų prisijungimo bei naudojamų kompiuterių veiksmų internete duomenys renkami ir saugomi serverių operacinių sistemų priemonėmis iki 30 dienų, jei kiti teisės aktai nenustato kitaip.

14.5. Informacinės sistemos naudotojų prisijungimo internete duomenys yra prieinami tik sistemos administratoriui ir gali būti atskleisti tik Administracijos direktoriaus raštišku nurodymu.

15. Prarasti, iškraipyti, sunaikinti informacinės sistemos duomenys atkuriami iš informacinės sistemos duomenų kopijų.

16. Informacinės sistemos duomenų kopijų darymo, saugojimo ir duomenų atkūrimo iš atsarginių duomenų kopijų tvarka:

16.1. Informacinės sistemos duomenų kopijos daromos į tam skirtą duomenų saugyklą, esančią kitoje patalpoje negu serveriai, kiekvieną darbo dieną po darbo valandų.

16.2. Kopijuojama ir saugoma tiek informacinės sistemos duomenų, kad duomenų praradimo atveju visišką informacinės sistemos funkcionalumą ir veiklą būtų galima atkurti per 1 darbo dieną, neskaitant duomenų kopijavimo trukmės.

16.3. Duomenų saugykloje yra saugoma ne daugiau savaitės senumo visų duomenų kopija ir skirtuminės kopijos, leidžiančios atkurti duomenis iki vienos dienos prieš gedimą.

16.4. Informacinės sistemos duomenų atkūrimo bandymai atliekami vieną kartą per metus.

16.5. Informacinės sistemos duomenų atkūrimo bandymai atliekami ne darbo valandomis ir prieš tai informavus visus informacinės sistemos naudotojus.

16.6. Už informacinės sistemos duomenų kopijų darymą ir duomenų atkūrimo bandymus yra atsakingas sistemos administratorius.

17. Pranešimų dėl neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo teikimo tvarka:

17.1. Informacinės sistemos naudotojas, įtaręs, kad su informacinės sistemos duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai sistemos administratoriui. Sistemos administratorius pagal informacinės sistemos posistemių įvykių žurnalų įrašus nustato įtartino poveikio šaltinį, laiką ir veiksmus, atliktus su informacinės sistemos duomenimis.

17.2. Sistemos administratorius nustatęs, kad su informacinės sistemos duomenimis galėjo būti atliekami neteisėti veiksmai, privalo apie tai pranešti Administracijos direktoriui ir saugumo įgaliotiniui.

17.3. Administracijos direktorius ir saugumo įgaliotinis, gavę pranešimą apie atliekamus neteisėtus veiksmus su informacinėje sistemoje tvarkomais duomenimis, inicijuoja Rokiškio rajono savivaldybės informacinės sistemos veiklos tęstinumo valdymo plane nustatytas informacijos saugumo incidento valdymo procedūras.

18. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką, priklausomai nuo konkretaus atvejo, derina IS administratorius.

19. Programinės ir techninės įrangos keitimo ir atnaujinimo įtakos vertinimo metu turi būti įvertinama pokyčių nauda, pagrįstumas, įgyvendinamumas, pokyčiams atlikti reikalingos sąnaudos, taip pat IS darbo sutrikdymo ar sustabdymo rizika, elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo pažeidimo rizika.

20. Programinės ir techninės įrangos keitimai ir atnaujinimai, galintys sutrikdyti ar sustabdyti IS 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 IS. Eksploatuojamų IS aplinkoje pokyčiai 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 IS aplinkoje.

21. Operacinių sistemų ir taikomosios programinės įrangos keitimai turi būti valdomi: planuojami ir ištestuojami.

22. Už operacinių sistemų ir taikomosios programinės įrangos keitimų valdymą atsakingas IS administratorius.

23. IS naudotojai privalo laikytis nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių, naudojamų informacinės sistemos naudotojų tarnybinėms ar darbo funkcijoms vykdyti naudojimo tvarkos:

23.1. 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;

23.2. iš informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpų išnešamiems mobiliesiems įrenginiams turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas ir pan.);

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

23.4.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;

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

24. Duomenų teikimas ir (arba) gavimas yra nustatytas sudarytose duomenų teikimo sutartyse arba duomenų teikimą ir (arba) gavimą nustatančiuose teisės aktuose.

IV. REIKALAVIMAI, KELIAMI INFORMACINEI SISTEMAI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

25. Sistemos administratorius yra atsakingas už prieigos prie programinių, techninių ir kitų informacinės sistemos išteklių organizavimą, suteikimą ir panaikinimą informacinės sistemos techninės ir (ar) programinės priežiūros paslaugų (toliau – priežiūros paslaugos) teikėjams.

26. Sistemos administratorius suteikia priežiūros paslaugų teikėjams tik tokias prieigos prie informacinės sistemos programinių, techninių ir kitų išteklių teises, kokios yra būtinos norint teikti priežiūros paslaugas.

27. Reikalavimai priežiūros paslaugų teikėjams ir jų teikiamoms priežiūros paslaugoms nustatomi šių paslaugų teikimo sutartyse. Paslaugų teikimo sutartyse turi būti nurodoma, kad:

27.1. paslaugų teikėjai, kurdami ar modifikuodami informacinės sistemos ar jos posistemių taikomąją programinę įrangą turi naudoti informacijos saugumo nuo nesankcionuoto poveikio sisteminei, taikomajai programinei įrangai ir patalpoms priemones;

27.2. informacinės sistemos ar jos posistemių taikomajai programinei įrangai testuoti turi būti naudojami testinių duomenų bazių duomenys.

27.3. paslaugų teikėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams, nustatytiems Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše.

28. Sistemos administratorius privalo supažindinti priežiūros paslaugų teikėjus su suteiktos prieigos prie informacinės sistemos saugumo reikalavimais ir sąlygomis.

29. Gavęs informaciją apie pasibaigusį sutarties su priežiūros paslaugų teikėju galiojimo terminą ar atsiradus kitoms informacinės sistemos saugumo politiką įgyvendinančiuose dokumentuose išvardytoms sąlygoms, sistemos administratorius privalo per 1 darbo dieną panaikinti priežiūros paslaugų teikėjui prieigą prie informacinės sistemos išteklių.
